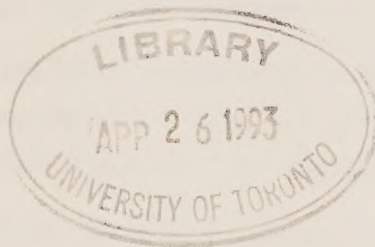


CAI
-1986
S71

Government
Publications



SUGGESTED CHANGES
TO CANADA'S 1982 PRIVACY ACT ©



by
Ken Rubin
68 Second Avenue
Ottawa K1S 2H5
Spring 1986

FOREWORD

In May 1986 public Parliamentary hearings to review Canada's 1982 Privacy Act will begin. These hearings will take place at a time when Canadians are more aware than ever of both their privacy needs and threats to their privacy. This report elaborates on some of the changes needed in the 1982 Privacy Act to provide privacy protection for the citizens of Canada. *

The time has come for parliamentarians to face the present and potential threats to personal privacy, such as those engendered by computer technologies. There is a clear need for legislation that goes beyond privacy access questions and protects our information privacy from technological abuses.

The report is divided into two parts. Part One deals with the limitations and inadequacies of the Privacy Act. Part Two briefly explores the reasons for, and components of, a more comprehensive privacy protection act.

The attached seven page summary of this report was made available to the parliamentary review committee in March 1986.

The analysis undertaken in the full report assumes the reader has some knowledge of Canada's Privacy Act as well as providing a more detailed framework for improving the Act.

Refer to my report Prying Eyes (1983) for a glossary of much of the Privacy Act's terminology. Readers are also advised to consult the Privacy Act itself, and the Index to the Act put out by the Privacy Commissioner's Office.

This report is dedicated to the betterment of the privacy protection of Canadians.

* The report was independently produced, without funding, and is a copyrighted publication of the author. Further copies may be obtained for \$25.00 plus delivery from the author.

TABLE OF CONTENTS

	Page
FOREWORD	
NOTE ON THE AUTHOR	
SUMMARY	
PART I: DATA PROTECTION CHANGES	1
CHAPTER I: ASSESSMENT OF THE PRIVACY ACT	1
CHAPTER II: LIMITATIONS ON INDIVIDUAL ACCESS TO PERSONAL INFORMATION	4
A. PRIVACY ACCESS RIGHTS	4
B. DENIAL OF ACCESS TO PERSONAL INFORMATION	6
CHAPTER III: INADEQUATE SAFEGUARDS TO PROTECT PERSONAL INFORMATION	16
A. NECESSARY COLLECTION OF PERSONAL INFORMATION	17
B. DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES	20
C. COMPUTER LINKING, MATCHING AND PROFILING	39
PART II: BEYOND PRIVACY ACCESS AND DATA PROTECTION - SUGGESTIONS FOR AN OMNIBUS PRIVACY PROTECTION ACT	52
A. BROADER PRIVACY CONCERNS	52
B. A GENERIC APPROACH	55
CONCLUSION	61
APPENDIX ONE - Need for a Periodic Report Card on the Operation of the Privacy Act	
APPENDIX TWO - Privacy Act Problems Formally Brought to the Privacy Commissioner's Attention and His Responses	



Digitized by the Internet Archive
in 2022 with funding from
University of Toronto

<https://archive.org/details/31761115513533>

NOTE ON THE AUTHOR

As a consumer researcher and advocate, I have been involved in a variety of privacy projects over the last decade.

As an advocate, I have participated in local and national civil liberties work in privacy invasion issues, including case counselling and helping to develop a citizen pamphlet on privacy.

I have made three appearances before parliamentary committees on privacy legislation matters:

1. As a consultant to the Canadian Rights and Liberties Federation in front of the Standing Joint Committee on Regulations and Other Statutory Instruments, February 15th, 1979, Issue 9.
2. As Chairperson of the Information Right's Committee, Civil Liberties Association, National Capital Region, on Bill C-43, in front of the Standing Committee on Justice and Legal Affairs, April 14, 1981, Issue 29.
3. As an individual witness on Privacy Act Regulations before the Standing Joint Committee on Regulations and Other Statutory Instruments, May 17, 1984, Issue 7.

As the Chairperson of the local Ottawa Civil Liberties Information Rights Committee, I presented a brief in May 1980 to the Privacy Commission's Inquiry on restricting the extended use of social insurance numbers.

I also participated in, and helped to design and organize, two privacy seminars in 1984:

1. A public seminar sponsored by La Ligue des droits et libertés of Quebec.
2. A workshop on various privacy and technology concerns for the Science Council of Canada.

I have been a speaker and panelist at various sessions on privacy, including the National Human Rights Coalition Conference in Ottawa in 1983, and the Ontario Government Privacy Conference in Toronto, in 1984.

I have also written a variety of reports and articles on privacy.

The first report, How Private is Private? (1978), largely dealt with personal experiences in using Canada's privacy access legislation, Part IV of the Canadian Human Rights Act entitled The Protection of Personal Information.

The second report, Prying Eyes (1983), reviewed problems with Canada's most recent privacy access legislation, the 1982 Privacy Act.

The third report, Essays on Privacy Invasion 1976-1984 (1985), dealt with a variety of privacy issues, from computer-matching to electronic monitoring of the workplace. These issues are especially relevant to enacting future privacy legislation.

I have written articles on privacy for The Canadian Encyclopedia, Perception, Info-Age and CUPE Facts.

I have actively monitored the 1982 Privacy Act and have reported problems to the Privacy Commissioner. * Although I have not applied for personal information under the 1982 Privacy Act, I gained relevant experience in 1978 when I accessed personal information held by various federal departments.

My experience as a Privacy Case Coordinator of the Canadian Rights and Liberties Federation, especially my experience in assisting the applicants in the Reyes and Ternette Federal Court cases, also proved to be helpful when it came time to preparing this assessment of the current Privacy Act.

* My correspondence with the Privacy Commissioner is attached as Appendix Two.

Laws don't stop prying by computer, says expert

Citizen
AP 11/8/86
PA10

The Canadian Press

Federal privacy laws offer Canadians little protection against electronic intrusions into their personal lives, a consumer researcher and advocate says.

"In my view, the Privacy Act needs more than a tune-up ... to meet the present and potential threats to personal privacy, such as those engendered by computer technologies," Ken Rubin states in a recent report proposing changes to the federal legislation.

The legislation was inadequate when it was proclaimed in 1982 and has been eroded since then by laws establishing the Canadian Security Intelligence Service, strengthening maintenance orders after divorce and helping collect federal employee debts, he said.

"Legalized snooping is a serious problem whose true dimension has yet to be measured," Rubin says in a paper prepared for a Commons committee review of the Privacy Act and the Access to Information Act.

The civilian security agency, which replaced the RCMP security service in 1984, was given sweeping powers to collect per-

sonal information through various intrusive means, including wire-tapping and mail opening.

Legislative amendments coming into effect later this year will allow the courts to track errant spouses who have failed to make maintenance payments and garnishee federal payments such as unemployment insurance and old age pensions to cover their debts.

Courts may also draw on federal information banks to find debtors employed by the federal government and then garnishee wages, tax refunds and pensions.

The privacy law was supposed to guard privacy while giving citizens the right to see what some government files say about them. But Rubin says it does more to help administrators than to control the collection and dispersion of personal information.

His 60-page report recommends amendments to ensure that the government gathers only relevant personal information and that no personal information files are kept secret.

As well, he says there should be tighter restrictions on third-party access to personal information.

Ken Rubin
68 Second Avenue
Ottawa K1S 2H5
Spring 1986

SUMMARY

Canadians are now very well aware of their privacy needs and are increasingly sensitive to threats to their privacy. This report proposes some changes to the 1982 Privacy Act which may be needed to provide more complete privacy protection for the citizens of Canada.

In my view, the Privacy Act needs more than a tuneup, or the addition of a stronger data protection authority, to meet the present and potential threats to personal privacy, such as those engendered by computer technologies.

The 1982 Privacy Act, as a data access act, offered some improvements to Part IV of the 1977 Canadian Human Rights Act, entitled The Protection of Personal Information. However, this second-generation privacy legislation does not address the problems of privacy invasion posed by electronic recording and surveillance. The Privacy Act, for instance, does not deal in realistic ways with various computer linking and matching practices. Broader privacy protection legislation would provide a tough preventive framework for dealing with the growing use of technology to invade our private lives.

The 1982 Privacy Act has primarily benefitted certain employee groups, inmates and government beneficiaries who want to gain access to files that would normally be difficult to obtain. The average Canadian, however, has not used the Privacy Act. This can be attributed to a lack of publicity and to public skepticism and disinterest.

Departmental reports on their Privacy Act operations have not contributed to the public's understanding of the potential uses of the Act. In sharp contrast, the Privacy Commissioner's annual reports have helped to raise the public's consciousness about the Act.

ACCESSING PERSONAL INFORMATION

The 1982 Privacy Act grants certain rights for obtaining access to personal information but also allows many exemptions and exclusions which are far too broad. The Act also gives many third parties access to personal information. A use and disclosure "code" is incorporated into the Act, but it provides only limited privacy safeguards. The Act lacks strong enforcement mechanisms for ensuring that only necessary personal information is collected. *

The Privacy Act has been undermined by the passing of several pieces of federal legislation, including the Canadian Security Intelligence Service (CSIS) Act, the Family Orders Enforcement Assistance Act, and an amendment to the Financial Administration Act. The new security legislation allows the civilian security agency to use almost every technique of personal privacy invasion, including computer-matching and mail opening. The new divorce legislation permits family maintenance defaulters, or individuals wrongfully holding their children in custody, to be electronically traced. The Financial Administration Act amendment enables garnishment of Crown monies owed delinquent federal employees after their whereabouts are traced. The security legislation even contains a clause amending the Privacy Act in matters that go beyond the purposes of that piece of legislation. **

EXEMPT DATA BANKS

The main legal change in the Privacy Act has come about through a Federal Court challenge to the validity of the "exempt data bank" concept in the Act. Exempt banks established by Cabinet consist of whole classes of personal information to which an individual cannot have access. They include, for the most part, information related

* For example, unlike the proposed Conservative bill in 1979, the current Privacy Act does not call for restricted uses of social insurance numbers.

** The CSIS Act removes the requirement for 18 investigative agencies, including CSIS, to place a notation on individual personal files indicating that they have accessed those files as third parties.

to matters of security and law enforcement. Nick Ternette, a Western Canadian activist, sought access to the exempt RCMP Security Services data bank and introduced successful legal arguments. It was his contention that the RCMP had not properly checked this exempt bank to determine if the files in it were restricted predominantly to personal information connected to security and law enforcement matters. *

The Privacy Commissioner, in his audit of the two immigration exempt banks, came to similar conclusions. The concept of exempt banks, therefore, may be quite misguided; the banks appear to have been set up primarily for administrative convenience without attending properly to civil liberty concerns.

A case-by-case review and application of security and law enforcement exemptions where appropriate, still apply in privacy cases, resulting all too often in the continued inability of individuals to access their files. However, the Ternette case firmly established that these types of denial of individual information are subject to judicial review. The federal government, until Justice Minister Crosbie's announcement, appealed the extent to which the Federal Court could permanently review cabinet-created exempt banks.

PERSONAL INFORMATION HOLDINGS

The Privacy Commissioner has not yet made full use of his audit powers to examine the various government personal information holdings in terms of their use and necessity. One department-wide compliance review has been done by the Commissioner in Fisheries and Oceans which is a department that lacks extensive personal information files. The Commissioner's findings turned up some problems in relation to the collection, description and use of personal information.

* Most of the other 20 exempt government data banks are probably improperly constituted. The act does not include provisions for a periodic review of such banks by Cabinet although the Privacy Commissioner has authority to audit exempt banks.

A review of some of the other exempt banks is underway as a result of the Ternette case. An audit has begun related to the departmental use of Section 8(2)(e) of the act. This section compels 18 investigative agencies to note their uses of federal personal information holdings by creating new personal information banks which are largely inaccessible to individuals but are accessible to the Commissioner.

The third edition of the Personal Information Index indicates the breadth of the government's personal information holdings, but it does not sufficiently identify all of the personal information holdings and it fails to clarify the ways that the approximately 140 agencies covered by the Act use these holdings.

THE PROVINCES AND THE PRIVATE SECTOR

The Privacy Act has not inspired most provinces to enact similar legislation. Quebec has the only operational privacy legislation, which is in many ways far superior to the federal act as a data protection measure.

The federal-provincial agreements on data-sharing, initiated by Justice Canada in 1983 and enacted without publicity, offers minimal safeguards and only defines in a vague way how and what information ought to be shared.

The Government has decided not to extend its principle of fair information practice to federally regulated industries. Further, the Government made only a weak effort to encourage the private sector to adopt the 1980 OECD privacy and transborder personal data guidelines only adopted by Canada in 1984.

THE PRIVACY COMMISSIONER

The Privacy Act is like a ship without a navigator. The Government has not publicized the Act. The Privacy Commissioner, while strong as an educator, has as yet not performed effectively in his audit-oversight role. The Commissioner has at times appeared

to favour the government rather than the user. This has not enhanced his credibility.

Yet the Commissioner has pinpointed the dangers to privacy posed by increasing storage of personal information on government micro computers, and by computer data linkages where personal information can be manipulated and used to create new personal information. Computer-matching is growing in Canada. It can be done without the individual's consent and without proper respect for full due process rights. In fact, it can be used as a tool to investigate certain groups.

INDIVIDUAL CONSENT FOR THIRD PARTY ACCESS TO PERSONAL FILES

Balancing the public's right to know against the right to individual protection from unwarranted privacy invasion is surfacing as a major issue. The problem remains that neither the Privacy Act nor the Access to Information Act has a defined residual balancing test that can be applied to weigh whether the right of access or privacy is paramount. Individual consent does not have to be obtained under the Privacy Act to release personal information in the public interest. There is considerable leeway for authorized third party access to personal information. The Privacy Act, after amendments introduced to it by the CSIS legislation, no longer has a requirement to note on individual files 18 investigative 'bodies' access. There is also no requirement for judicial warrants to be issued to approve each case of all investigative agencies' access to personal files.

A PRIVACY PROTECTION STRATEGY

Canadians, I suspect, would prefer a broad preventive approach to privacy protection - one that deals with both public and private sector privacy invasion problems in clear and effective ways.

A broader privacy protection strategy would deal with privacy invasion problems such as:

- . search and seizure
- . close electronic monitoring of the workplace
- . wiretapping and eavesdropping
- . third party access to mail
- . the use of lie detectors
- . computer-matching
- . the transfer of consumer funds electronically
- . interactive communications profiles.

A three-person Privacy Commission should be established to handle the workload. It must have regulatory clout. The Commission should have mediation powers. Where mediation does not resolve matters, it should have the power to enforce orders. The Commission should receive public input on privacy problems and monitor and audit practices of privacy protection in both the public and private sector.

The Commission should be the licensing authority for public and private personal information holdings. It should work hand-in-hand with industry, labour, and the media and others to create privacy protection codes in these sectors.

The Commission should also be accountable to Parliament. A designated parliamentary committee should receive the Commission's annual and special reports and then assess the privacy implications of all proposed federal legislation.

Individuals must also be actively involved in the protection of personal privacy. Governments can enable individuals to play responsible roles by enacting an omnibus privacy protection statute, for example, confirming the rights of individuals to sue and claim damages for invasion of privacy.

The enactment of a constitutional right to privacy would also provide individuals with a clear legal framework for protecting their personal privacy. *

Rapid advances in computer-related technology and the resulting threats to personal privacy cannot be adequately dealt with by the 1982 Privacy Act. We need to create generic privacy legislation. By that I mean all encompassing legislation that covers all aspects of privacy protection in Canada. Legislation that asserts our privacy rights can be enhanced by a broader preventive approach and by including more effective redress mechanisms.

There is also a pressing need to ensure that a revised Privacy Act will be reviewed periodically, since legislation tends to lag behind the development of technology.

The time has also come to create a separate Parliamentary committee to work exclusively on privacy issues.

Establishing public policies to deal with privacy protection is now an urgent matter; it is one very important factor in the continued evolution of individual-government relations.

* Some observers believe that Section 7, "Everyone has the right to life, liberty and security of person and the right not to be deprived thereof except in accordance with the principles of fundamental justice", and Section 8, "Everyone has the right to be secure against unreasonable search or seizure", of the 1982 Canadian Charter of Rights and Freedoms will be interpreted as privacy rights. My preference would be for a clear and unequivocal constitutional amendment on the right to privacy. The Quebec Charter of Human Rights has a rather specific article on privacy that reads as follows: "Every person has a right to respect for his private life".

PART I: DATA PROTECTION CHANGES

To improve the limited data protection section of the Privacy Act, the following provisions must be incorporated:

- . Greater individual control over what personal information can be held by federal authorities
- . Collection of necessary personal information only
- . Fewer and more narrowly defined exceptions to the right of access
- . Strict safeguards governing third party use of personal data
- . Civil and criminal penalties for unauthorized access to personal data
- . Registration and regulation of both public and private sector information under federal jurisdiction
- . A clearer right to correct erroneous information.

CHAPTER I: ASSESSMENT OF THE PRIVACY ACT

The 1982 Privacy Act, a second-generation data access act, does not give Canadians adequate privacy protection. * The Act includes several improvements over its 1977 predecessor, such as greater powers for the Privacy Commissioner, the addition of judicial review in certain cases when information is denied, and an extension of provisions for privacy protection to all federal personal information holdings of about 140 federal agencies. But, as this

* Canada's first attempt at privacy access legislation was Part IV of the Canadian Human Rights Act, entitled Protection of Personal Information. This legislation was passed in 1977.

researcher pointed out in his 1983 report, Prying Eyes, the 1982 Privacy Act has several significant weaknesses:

- . It misses the opportunity to strongly protect personal information against computer linking and personal data manipulation in the public and private sectors
- . It provides a weak use and disclosure code for federally held personal information
- . It permits too much third party access to personal information
- . It increases rather than decreases the number of exemptions that can prevent individuals from gaining access to their own data
- . It perpetuates the notion of whole personal information banks being exempted by Order-in-Council
- . It continues the trend of developing privacy regulations and directives without public input.

After writing the Prying Eyes report, this researcher actively monitored the Privacy Act and found the following problems with its implementation:

- . Parliamentarians have passed other pieces of legislation related to the debt collection of federal employees, divorce, and security intelligence, which have effectively undermined the spirit of privacy protection contained in Section 2 of the Privacy Act
- . Publicity about the Privacy Act has been negligible despite some good efforts by the Privacy Commissioner
- . Most Canadians have shown a high degree of skepticism and disinterest in the Privacy Act. The Act's main users include certain public employees, especially those in the Department of National Defence and the RCMP, inmates at federal penitentiaries, and recipients of federal social assistance benefits

- . Few audits on the necessity of Ottawa's personal information practices have been conducted and very little information has been reported in the annual privacy report of departments related to individual and third party use of personal information banks
- . The annual Personal Information Index, although a useful guide, still does not adequately list many personal information holdings of the agencies covered by the Index
- . The Privacy Commissioner has proven to be an advocate on certain privacy problems such as computer-matching and the reluctance of provincial governments to release certain types of personal information. But he has, at times, chosen not to see his role as that of an ombudsman, offering support to individual complainants. This was the appearance given, for example, in the Reyes case. *
- . A minimal effort has been made by the government to convince the private sector to adopt the voluntary OECD privacy and transborder data guidelines
- . The increase in computer-matching and profiling has not received sufficient public debate and has not been subject to adequate guidelines
- . The concept of totally exempt banks has not been fully discredited, even though Nick Ternette, a Western Canadian activist who sought his RCMP security service file, succeeded in getting the Canadian Government to admit that this particular bank had not been properly validated.

* Reyes, a Chilean refugee, wanted to find out why he was being denied Canadian citizenship. The Privacy Commissioner indicated to the Secretary of State that the government had cited the wrong exemption to deny Mr. Reyes access to his records. In this way, the Commissioner appeared to side with the government. Mr. Reyes, since the Commissioner and Federal Court rejected his appeal to see his citizenship application files, has now been granted Canadian citizenship after his application for citizenship was reviewed further by the Canadian government.

CHAPTER II: LIMITATIONS ON INDIVIDUAL ACCESS TO PERSONAL INFORMATION

A major purpose of the Privacy Act, as outlined in Section 2 of the Act, is to safeguard an individual's right to access personal information held by the government. The Act fails considerably to meet this objective.

A. PRIVACY ACT ACCESS RIGHTS

Privacy Act access rights are limited by procedures embodied in the implementation of the Act, and by a lack of publicity to make citizens aware of their rights. Some suggestions regarding how to improve privacy access rights by moving beyond the provisions granted under the Privacy Act are listed below. The suggestions relate to improvements in the scope, procedures and awareness of Privacy Act rights.

Scope of Privacy Act Access

Use of the Privacy Act is limited to Canadian citizens and landed immigrants. As well, only about 140 federal agencies are currently covered by the Act and no federally regulated private sector companies are covered. To improve the scope of privacy access,

- . Access should be accorded to all individuals, regardless of their nationality
- . Access should extend to all federal government agencies
- . Access should include federally regulated private sector firms and access rights should be stated as part of contracts for those private sector firms receiving federal contracts and other benefits.

Privacy Act Access Procedures

Problems in terms of time delays, the correction of files, and the uncertainty associated with not knowing whether fees will

be assessed, can detract from access rights. To improve this situation,

- . Access should be granted within 20 working days subject to penalties imposed thereafter *
- . Access complaints should be handled within 30 days by the Privacy Commissioner's Office (and then sent to the Federal Court if necessary)
- . The process for correcting information should be made less cumbersome so that an applicant can file a statement of correction, and where a correction statement is unacceptable to the government, take the matter to Court. This should include having the Court order that deletions be made to the unacceptable file
- . It should be clearly stated in the legislation that access should not require any fees, and, that court challenges should not result in costs being assigned to applicants.

Awareness of Privacy Act Access Rights

The potential means of increasing the public's awareness of access rights include:

- . Developing concrete programs to better inform and educate Canadians about their Privacy Act access rights
- . Providing support to citizens clearinghouses to assist Privacy Act users.

* The majority of complaints viewed by the Privacy Commissioner are time related; the solution lies in tightening up the time given to process a case and in penalizing tardiness. Penalties assessed public officials and agencies would go to their victims.

B. DENIAL OF ACCESS TO PERSONAL INFORMATION

Access can also be denied when personal information on Canadians is exempted from individual access by the Act. This denial occurs for various reasons: i) the personal information is contained in totally exempt banks; ii) the information is inaccessible because of formal exemptions or exclusions; or iii) the information is inaccessible because of other types of subtle exemptions.

There are an estimated 300 million files that were identified in the 1983 Personal Information Index. Another estimated 200 million federal files are not covered in the Index, partly because some federal agencies are not covered under the Privacy Act but also because agencies covered under the Act have not calculated or listed many of their files containing personal information. Conservatively speaking, there are about 2 million estimated files that can be formally exempted under the 20 exempt banks and formal exemptions. *

It is interesting to note that over one in five of the 63,000 applicants to date have been refused total or partial access to their records given the Act's many legal exemptions and exclusions. Over one in ten applications cannot be processed for a variety of administrative reasons (eg. does not exist, insufficient information, abandoned etc.).

1. Exempt Banks (Section 18 of the Privacy Act)

Section 18 permits agencies to propose to Cabinet that they be allowed to exempt permanently, certain banks of personal information which relate to sensitive law enforcement and security personnel matters. Twenty such banks presently exist. They likely hold about 1.5 million files on Canadians. **

* Refer to Prying Eyes (1983), page 26.

** Ibid. pages 20 to 26.

In January 1984, after complaints were made to the Privacy Commissioner, this researcher called for an investigation of four separate matters related to exempt banks:

- . The creation of exempt banks for administrative convenience by Cabinet without any sunset provision. This is a violation of the Section 2 spirit of the Privacy Act, which implies that no permanent secret files should be kept on Canadians
- . The failure of the Communications Security Establishment Agency (CSE), a super secret agency, to create an exempt bank for eavesdropping records on Canadians' conversations
- . The questionable reasons for allowing two banks, the Canada Post Corporation's postal crime bank and the National Defence's military policy investigation bank to qualify for total exempt bank status
- . The exclusion of the number of files held in 16 out of the then 19 exempt banks.

The Privacy Commissioner responded on July 9, 1984 with the argument that he had "no authority to receive and investigate complaints against the designation of a personal information bank as exempt" and that "there is no requirement in the Privacy Act that the number of files held in exempt banks be specified". The Commissioner had already acknowledged on May 4, 1984, that National Defence was "taking the necessary steps to list a personal information bank maintained by CSE in the next (1985) publication of the Personal Information Index". *

The Privacy Commissioner in the Ternette case (and other cases dealing with complaints about exempt banks) said that his powers were limited. ** However, in the Federal Court review of

* This vaguely worded exempt bank is found on page 60-3 of the 1985 Personal Information Index.

** Nick Ternette wanted access to the RCMP security services bank which had been designated an exempt bank and his complaint was initially rejected by the Privacy Commissioner.

the Ternette case, the presiding judge ruled that exempt banks were subject to full scale judicial review. With the change of governments, the Conservatives dropped the appeal of this matter. Further, the Department of Justice conceded that Ternette's argument was valid; the RCMP Security Service bank had not been properly constituted (and hence the Privacy Act had been violated) because some several hundred thousand files had not been vetted to see whether they consisted predominantly of personal information described under Section 21 or 22 of the Privacy Act.

The Privacy Commissioner, under Section 50 of the Act, has the power to bring to the Court's attention any cases where an exempt bank has been improperly claimed. As a result the Commissioner has, at the initiative of Ternette, re-entered the case.

It is unlikely that Ternette will ever be told whether he has a file in the RCMP Security Services bank. It is even more unlikely that he will be able to see his file if it does exist. Nevertheless, Ternette has helped to challenge the validity and necessity of exempt banks. The Commissioner has yet to report his findings and hence the Court case is still active.

Some agencies including the RCMP, with its criminal intelligence exempt banks, and Revenue Canada - Taxation, with its tax avoidance and evasion exempt banks, still firmly claim that their exempt banks are properly constituted and regularly vetted.

The results of the Privacy Commissioner's audit of the two exempt immigration banks that this researcher obtained under the Access to Information Act, stand as further evidence in support of changing the system of exempt banks. The Commissioner found that these banks had not been properly established, although Employment and Immigration disputes this finding.

Two possible solutions to the problem of exempt banks are as follows:

- . Abolish exempt banks so that whole classes of personal information cannot be considered exempt

- . Restrict the breadth of Section 21 (international affairs-defence) and Section 22 (law enforcement) and ensure that a "substantive injury" test is applied to all cases where Sections 21 and 22 has been cited.

2. Formal Exemptions (Sections 19 to 28 of the Privacy Act)

Formal exemptions under the Privacy Act are numerous and broad in scope. Section 19 (other governments' confidential submissions), Section 20 (federal-provincial affairs), Sections 21, 22 and 25 (safety of individuals), and Section 27 (solicitor-client privilege), are quite similar to exemptions in the Access Act. Section 23 (security clearances), Section 24 (non-disclosure to individuals sentenced for an offence), Section 26 (information about another individual), and Section 28 (medical records) are unique to the Privacy Act. Generally speaking, exemptions claimed in the Privacy Act should be:

- . Better defined and reduced in number
- . Discretionary on a case-by-case review basis, not mandatory as they are under Sections 19 and 22(2)
- . Subject to harms tests, rather than sweeping class exemptions like Sections 19, 22(1)(a), 23, 24(b), 26, 27, and 28.
- . Subject to full scale judicial review, unlike Section 49 that limits the review to "reasonable grounds" for Sections 20, 21, 22(1)(b) and (c), and 24(a)
- . Time-restricted with identifiable retention and disposal schedules

To be more specific, two formal exemptions, Sections 19(1) and 28, are discussed in greater detail below.

2. Section 19(1) (Treatment of Other Governments' Confidential Data)

Access to personal information can be totally denied under Section 19(1). For example, this section protects international,

provincial, and municipal confidential information. Treasury Board statistics show that almost 20% of all those Privacy Act applications which are subject to exemptions, are denied personal information on the grounds of Section 19.

In 1984 this researcher used the Access Act to discover that at least 8 provinces or their agencies had made some claim to 12 federal departments asking that the personal information they had submitted be considered confidential. The blanket nature of Section 19(1) has been criticized by the Privacy Commissioner. For instance, it prevents federal employees from gaining access to their provincial medical file claims covering worker's compensation; files they need access to in practice. Section 19(1) should not remain mandatory. Decisions regarding the release of information ought to be made on a case-by-case basis. A harms test as to why release would be injurious to the State's interests or the individual's interest should be introduced.

Section 28 (Medical Records)

Section 28 was added to the 1982 Privacy Act to ease the work of government administrators. This resulted in a neglect of the paramount right of individuals to control the release of records which might affect their day-to-day lives.

Section 28 makes provision for the State to decide which health records can be released to individuals. The State defines the proper physical and mental health requirements in individual case releases or denials and relies in part on professional medical people - some of who may be government employees - to make these decisions.

Denying sensitive medical records is not the job of the State. About 5% of the Privacy Act applications which are subject to exemptions are denied medical record information. Individuals should have access to their own medical records, especially in situations when the individual's own health advisor is present when the information is released.

3. Subtler Exemptions Under The Privacy Act

Formal exemptions and exempt banks are not the only means of keeping personal information secret. The following list describes other parts of the Privacy Act which contribute to the maintenance of a high degree of secrecy.

- . Under Section 70 personal information contained in cabinet confidences is excluded for 20 years. Personal information in cabinet discussion papers is not always accessible. There is no judicial review
- . Under Section 16(2) the government can deny the existence of personal information files. This is not just limited to sensitive security files. Over 5% of Privacy Act users are informed that no records exist; it is difficult to know, however, exactly how many of these instances involve Section 16(2)
- . Section 3 lists about 140 federal agencies as falling under the provisions of the Act; access to personal data from other federal agencies not listed in the Act's Schedule is therefore excluded *
- . Under Section 12(1) non-landed immigrants and foreign nationals cannot apply for their personal information unless they are federal prison inmates from other countries as proclaimed by cabinet under Section 12(3). It is inconsistent to permit one group of foreigners access to records while not extending the right to others
- . Under Section 8(2)(g) it is possible for a Member of Parliament (and Crown Ministers are M.P.'s) to obtain access to an individual's personal information to assist that individual in resolving a problem. The affected individuals, however, cannot then necessarily gain access to this information held by the Member of Parliament

* This has been controversial. For instance, releasing salaries of order-in-council appointees from non-listed crown corporations does not technically have to be done.

- . Under Section 8(2)(e) and Section 9 as amended by the CSIS Act, individuals who obtain access to their files will no longer be able to see whether one of 18 named investigative agencies have investigated them. Section 89 of the Canadian Security Intelligence Service Act removed the personal file notation system for these 18 agencies when they made use of these files. *
- . The Privacy Act does not include a severability section, like that in the Access Act. Only in Treasury Board directives are departments encouraged to provide personal data that can be practically severed from general information. **

In the light of these kinds of exemptions, the following amendments ought to be made to the Privacy Act to improve access to personal information.

- . The severability principle should be introduced
- . All non-landed immigrants, foreign nationals and individuals without a national passport, should be allowed to apply under the Act
- . All federal crown corporations and other agencies should fall under the provisions of the Act

* Refer to media stories for an elaboration of this point (Globe and Mail February 24, 1985; Ottawa Citizen February 25, 1985; and Toronto Star February 26, 1985). Law enforcement agencies pressed for this change, arguing that individuals should not know who accessed their files for investigative purposes. Under Section 8(4) investigative agencies must make note of the times they access specially created personal information banks. Yet, this notation is made for the benefit of the Privacy Commissioner should he need to or choose to review the file; it is doubtful that individual citizens will ever gain access to these information banks.

** The Privacy Act refers to "information" unlike the Access Act which refers to "records" and, hence, the severability principle may not technically be needed. However, in practice, some departments are having problems severing requested personal information from general files where exemptions apply or where the files contain information about more than one individual.

- . MP and Ministerial files of personal information related to individual case assistance under federal programs should become accessible
- . Cabinet confidences should be granted and claims for cabinet confidentiality should be made the subject of judicial review
- . It should no longer become possible to deny the existence of records in all cases, except where a court order for security intelligence reasons is issued
- . Individuals should again be given the right to know which third party investigators under Section 8(2)(e) have accessed their individual files (except where the court, in security intelligence cases, orders otherwise).

Even subtler types of exemptions exist. These exemptions are created under three different sets of circumstances: the failure of citizens to exercise their privacy access rights due to poor government assistance and publicity; the inadequate identification of government information holdings; and the application of exemptions to personal information which derive from other acts of parliament.

(i) Improper Assistance and Poor Publicity

Treasury Board statistics show that almost 2% of Privacy Act applications are abandoned. Almost 3% lack sufficient information, and 1½% cannot be processed.

There are many reasons for these failures, but one important issue is whether government assistance efforts are adequate to help the public to follow through on their Privacy Act requests.

Equally hard to determine is the number of individuals who have never heard of the Privacy Act and who are thus deprived of their privacy access rights because of the government's poor publicity efforts.

The Privacy Act must be modified so that it publicizes privacy rights and helps Canadians to exercise these rights. This kind of change could include providing support to community-based organizations such as civil liberties groups, so that they can assist individuals and initiate public discussion about privacy protection.

(ii) Inadequate Identification of Federal Personal Information

About 2200 federal personal information banks are identified in the Personal Information Index and are retrievable by name or through some identifying number or symbol.

However, not all of the information held by the some 140 federal agencies covered under the Privacy Act, particularly those involving "classes of personal information" under Section 19(1)(b), is sufficiently identified in the Index.

In fact, fewer and fewer departments are bothering to list the number of files held per personal information holding. A sense of the size of personal institutional holdings is an important part of the public's right to know about how the government operates. This researcher estimates that there are at least 300 million reported files in the Personal Information Index and another 200 million files that go unreported. The lack of proper identification of information holdings causes public skepticism.

The Privacy Commissioner, on August 10, 1984, in response to this researcher's complaint about the Personal Information Index, said that the Index would be gradually improved as discrepancies and deficiencies are discovered. But this does not solve the immediate problems of sloppy record keeping practices, and the desire of some officials to refrain from revealing the existence of records. These are matters which go beyond improving descriptions in the Personal Information Index. *

* One major institution, Justice Canada, is still rated as unacceptable in an October 1985 Treasury Board Study, in terms of its Personal Information Index and Access Register descriptions. Justice is the agency that has policy responsibilities under the Privacy and Access Acts.

The Privacy Commissioner did recognize in his 1984-85 Annual Report that, with the advent of micro-computers, it will become harder to keep track of all federal personal information holdings. Treasury Board has yet to issue a directive to departments on how best to organize their electronic data processing files.

(iii) Exemptions from Other Acts of Parliament

A further point needs to be made about the exemptions to personal information which are possible under the Official Secrets Act, under Section 36.2 of the Canada Evidence Act and the proposed Archives Bill C95. These pieces of legislation's security provisions provide much broader definitions of security than is found in Section 21 (international affairs and defence) of the Privacy Act. There ought to be greater consistency in the scope of exemptions and a clear statement in the Act which, if any, laws supercede or override the Privacy Act. Canadians would like to forget such cases as the Peter Treu case and the issues that it raised. *

4. A Final Note on Exemptions

The Privacy Act has many types of exemptions and ways of creating secret information. Moreover, some pressure exists within public agencies, particularly law enforcement agencies, to broaden existing exemptions, for instance, there is some pressure to make more whole classes of personal information exempt; and to promote a policy advice exemption, similar to the one in the Access Act, such that information related to the way public employees handle personal situations will be exemptable for up to twenty years.

The only formal system of recourse for trying to gain access to information which has been denied under the Privacy Act is to complain to the Privacy Commissioner, and then, where necessary, to appeal to the Federal Court of Canada.

* Peter Treu was prosecuted under the Official Secrets Act for reputedly leaking information related to NATO's secret air defence communications system. After secret court proceedings and much pressure, the charges were dropped.

No penalties are presently assessed for damages that can be claimed for wrongful denial. Stiff fines of up to \$10,000 should be assessed to ensure the widest possible access rights.

It is difficult to place a value on personal information or to determine how much personal information is withheld because it is sensitive to the State. But it is clear that members of the public are not being served well by the Privacy Act, which is biased in favour of the interests of governments and public agencies.

CHAPTER III: INADEQUATE SAFEGUARDS TO PROTECT PERSONAL INFORMATION

The Privacy Act is much more than legislation aimed at giving individual access to personal information. The Act's Section 2 purpose clause also states that the act attempts to protect the privacy of individuals with respect to personal information held by the government.

The three basic problems with the protection system under the Privacy Act are as follows:

- . The Act is designed more to suit administrative convenience than to ensure the interests of individual privacy and control over personal information. Personal information collection may not always be necessary or with individual consent
- . The Act offers a weak preventive third party, use and disclosure code without sufficient remedies, penalties or means of enforcement

- . The Act does not effectively prevent the use of computers to manipulate and link personal information.

A. NECESSARY COLLECTION OF PERSONAL INFORMATION

The Privacy Act does not adequately provide answers to the following questions about the personal information that government agencies collect and store:

- . Is the information necessary?
- . Is the information collected with the consent of individuals?

Section 4 of the Privacy Act states that personal information is only to be collected if "it relates directly to an operating program or activity of the institution". This begs the question of whether, for instance, questions on the long census form need to be asked or answered. * Individuals are not being given sufficient information or opportunity to object to providing personal information. **

Part of the problem lies with the manner in which the Privacy Act is written. The Act does not clearly require individual consent for most of the individual information collected by government. Instead, the Privacy Act allows the government to "inform" individuals about the purposes, however vague and unnecessary they may be, that such collection serves. Individuals are not always informed in clear language that they do not have to fill out all of the information that the government requests from them.

* A Vancouver area woman in December 1983 was acquitted by a British Columbia provincial court for refusing to answer census questions such as the number of bathrooms in her house. A 1984 appeal by Justice Canada was not successful.

** One novel feature of the Conservative privacy bill proposed in 1979 was that no penalties or withheld benefits would apply in cases where individuals refused voluntarily to provide their social insurance number information. The bill was not introduced before the Conservative government's defeat.

Also, while the federal government claims in Section 5 of the Act that it will try to collect information directly from individuals, this does not imply the government's intention to gain individual consent or to, in fact, collect the bulk of personal information directly from individuals.

Only one concession is made under Sections 6(1) and 6(3) of the Privacy Act. Before a unilateral government decision is made to dispose of personal information holdings (either by destroying them or considering them as archival material), a "reasonable opportunity" must be given to individuals to obtain access to the data which was used for an administrative purpose. Record retention and disposal schedules are still not all set out in the Personal Information Index and the only formal method of challenging these schedules is by complaining to the Privacy Commission:

The only audit carried out by the Privacy Commissioner to date on the personal information collection and storage practices of the federal government was his 1985 Fisheries and Oceans department audit. Even in this department, with its relatively minor personal information holdings, the Commissioner found some personal information holdings that were not necessary for administrative purposes. He also discovered that not all of these holdings had proper retention schedules or were properly identified in the Personal Information Index. The audit report, however, which was obtained only because Fisheries and Oceans released it, made recommendations which were not compulsory for Fisheries and Oceans to adopt.

The Privacy Act requires amendment to reflect the following important privacy protection principles:

- . Under a revised Section 5 of the Act, only relevant personal information should be collected. The onus, however, to prove that there is a need for collecting such information, should still lie with the government

- . A standard, personal information form should be developed to provide guidance on the acceptable means of collecting personal information and that provides clear instructions to individuals on how to specify the way they want their information to be treated *
- . No personal information holdings should remain secret under a revised Section 2 of the Act
- . Annual descriptions of personal information holdings under a revised Section 11 of the Act should include the number of individual files being held; a full description of the individual data in the files; the specific recording, retention and disposal practices followed by the government; the specific ways the government plans to use the data; details of specific third parties who have access to the data; and the guidelines that third parties must follow when accessing the information
- . The Privacy Commission should have powers under a revised Section 37 of the Act to order changes in departmental personal information descriptions, practices and guidelines
- . As well, all audit reports and recommendations made by the Privacy Commission should be made public upon their completion. Agencies should have a 60 day period to prepare a public response, including a timetable and plan of action and verification of any consequent changes should then be prepared and immediately made public by the Privacy Commission
- . The Privacy Commission should also have the power to impose penalties for inconsistent information usage and improperly registered information banks. **

* Treasury Board's model suggested statements inadequately inform individuals about their rights in terms of personal information collection, and its forms do not tell individuals to note down their consent or refusal for information release. The wording of Section 5(2) of the Act will have to be changed to reflect these collection requirements.

** Treasury Board has a statutory role (Section 71) to ensure the proper registration of departmental personal information banks, both existing ones and new ones, but has no real powers to penalize departments for improper registration.

B. DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

The Privacy Act's use and disclosure practices codified in Sections 4 to 8 of the Act are primarily designed for administrative convenience rather than for privacy protection. The Act provides rights of third party disclosure without sufficient preventive safeguards for affected individuals; it does not prohibit disclosure unless absolutely necessary and under strict guidelines.

The considerable leeway for authorized third party access to personal information in the Privacy Act helps to destroy the spirit of protecting individuals from unwarranted privacy invasion.

Administrative Use of Personal Information

The problem of third party access to personal information begins with the self-serving manner in which personal information is treated in the Privacy Act.

The Privacy Act has the following three weaknesses in the area of personal information use:

- . Personal information is predominately controlled by government institutions themselves, rather than by the individuals who give information about themselves to the government, or who have had information collected about themselves without their knowledge
- . Vague clauses about "the purpose for which information was obtained or compiled by the institution or for a use consistent with that purpose" provide broad ranging administrative authority to use personal information based on the following conditions: a) information can be used without usually receiving individual consent and without necessarily referring to specific Acts of Parliament; b) information can be used on the understanding that such consistent uses are supposed to be publicized previously in the Personal Information Index (Section 11(1)(a)(iv)); and c) information can be used with the approval of the

Privacy Commissioner when the personal information use differs from the consistent norm. All that has to be done according to Section 9(3) is to list the new consistent use in the next Personal Information Index.

- . The administrative use of personal information is approved if it is "consistent" (Section 7(a)) and not because it is clearly authorized under Acts of Parliament or regulations (Section 8(2)(b)). Conveniently, there is no real definition of "consistent". The administrative process in too many instances becomes the purpose and raison d'être for justifying weak privacy protection.

To tighten up the Act in terms of information use this author recommends the following three amendments:

- .. Personal information usage should be authorized by specific parliamentary acts and regulations
- . These acts and regulations (somewhat like the Access Act provision of Section 24(2)) should be reviewed by the designated parliamentary committee by the end of 1987 to see whether they are consistent with a revised Privacy Act *
- . Adequate monitoring mechanisms should be put in place to assess how public employees use personal information under acts of parliament. Many statutes should restrict their "fishing expedition" powers to collect almost any personal information (eg. Income Tax Act) and should offer greater assurances that necessary personal information is truly safeguarded and accessible to affected

* Justice Canada, in answering a 1983 Access Act request, stated that only 14 federal statutes had been identified with statutory provisions authorizing disclosure of personal information. The Personal Information Index, however, contains hundreds of examples of the collection and uses of personal information by officials are not referenced by statute.

individuals, unless revised and restrictive exemptions apply under the Privacy Act. *

The Privacy Commissioner in his July 9, 1984 response to this researcher may be right that there is no requirement in the Privacy Act to list federal statutes under Section 8(2)(b). But, this gap allows the distinction between so-called "consistent" use and legal authorized use to be further blurred.

Sections 7, 8(1)(2)(a) and (b) of the Act should be redrafted so that an institutional use of personal information code can be added - and one that is not self-serving to the federal bureaucracy. Further, Sections 8 and 9 should not change the content of Section 2 with the effect of implying that personal information held by government institutions ought to be controlled by them unless they can cite specific legal authority in Acts of Parliament. The control of personal information needs to be in the hands of the individuals who provided it -- the principle here is that individuals own any information about themselves.

Authorized Third Parties

Third party access is not only guaranteed through the administrative use provisions of the Privacy Act. It is clearly endorsed in the long list of authorized third parties, from public employees to Members of Parliament to law enforcement and investigative personnel, who, under Section 8(2) of the Act, can have access to personal information with very few exceptions.

* In 1984, in one case of complaint against Revenue Canada's thwarted plans to use various financial data bases from the City of Kitchener, the Privacy Commissioner found that the broad scope of the Income Tax Act did not make such potential uses of the personal data illegal (although they should be listed in the Personal Information Index). A Supreme Court judgment (the 1984 James Richardson and Sons Ltd. versus The Minister of National Revenue case ruling 1 S.C.R.614), however, found that Revenue Canada's search and seizure powers were too far reaching and should be restricted.

Public Employees as Third Parties

Sections 8(2)(a) and (b) allow many public employees, often without clearly designating specific senior individuals within organizations, sweeping access to individual personal information, reputedly because the administrative purpose allows such access. For example, there are many investigative bodies with access to personal information under Section 8(2)(a) and (b). But such law enforcement agencies are not clearly identified in the 1982 Privacy Act.*

Statutory authority rather than administrative directives should become the basis of third party access. Statutes must restrict the purposes of such entry to personal files to specified individual public employees who would then become accountable for their use of personal information. Any sharing of such personal data among departmental branches or other federal agencies should have statutory authority and be based on publicly identified data-sharing agreements that spell out guarantees to privacy protection and are listed in schedules in the Act. Individuals should have clear and precise knowledge of such third party access and be able to complain about its use or sue when there is a gross misuse of powers.

Family Orders Enforcement and Personal Information

The difficulty in controlling third party access to individual files can be illustrated by the latest attempt, through separate statutory authority, to improve the Privacy Act's use and disclosure code provisions. The case in point is the 1985 passage of the

* The draft Conservative 1980 Bill C15 had allowed for the identification of such investigative agencies in the schedule of its proposed access legislation. This researcher applied under the Access Act to obtain from Justice Canada the preliminary lists for investigative agencies which were to be incorporated under Bill C15.

The lack of a specific listing of investigative agencies under Section 22(2)(a) and (b) of the Privacy Act was brought to the Privacy Commissioner's attention as a problem for clearly knowing who these agencies were that could use personal information. The Commissioner's July 9, 1984 response was that "There is no basis in law to compel any government department to provide a complete list of the investigative agencies..."

Family Orders Enforcement Assistance Act as part of the divorce legislation. In this case, federal officials tried to limit the electronic tracing of defaulting spouses and wrongful child custody, partly as a means of limiting privacy invasion. The officials argued that the privacy protection provisions as follows are adequate:

- . Only in limited situations (eg. with court orders) shall the federal government proceed to trace targetted people
- . Provinces should first agree to designate personal information banks that can be used for tracing an address (drivers' licences and health record information for example)
- . Federal banks that can be tapped for tracing shall be limited to the five personal information banks of Health and Welfare and Employment and Immigration. These banks are two Canadian Pension Plan (CPP) banks, the Social Insurance Number (SIN) bank, and an employment and unemployment record bank
- . There should not be any linkages between the above named federal banks to trace people's addresses and the personal information banks that give out data on the federal monies to be seized for non-payment of family maintenance (eg. income tax refunds, Canada Savings Bonds interest, UIC, CPP, Old Age Security, Manpower Training Income, GIS and certain agriculture stabilization payments) *
- . Separate personal information banks should be created on the data that is collected as a result of tracing people and seizing monies.

* Provinces have always tried to monitor family maintenance payments, but only Manitoba has adopted an electronic monitoring system which has benefits in terms of speed in detecting default in payments and speed of action to correct this situation.

The fact remains, however, that privacy invasion is to some extent legally sanctioned and there are several loopholes which provide for further entry into personal information banks. Some of these loopholes are listed below:

- . Other Health and Welfare and Employment and Immigration personal information banks can be added by regulation - additions to the banks of all other departments require legislative enactment
- . Taxation files are not listed as a source of tracing but the CPP bank does contain a portion of the tax records pertaining to CPP
- . One of the five selected banks, SIN, can be used as the basis for linking a great deal of personal information. The five selected banks hold a great deal of information on individuals
- . The provinces can designate all or a specific number of their personal information holdings, although this is presumably a controversial matter which will have to be discussed at great length in the provincial legislatures before being approved
- . The list of what federal monies can be seized is only partially mentioned in the news release that accompanies the enforcement legislation, and no draft regulations specifying the breadth of such entry into personal financial banks has yet been tabled in Parliament
- . The claim that there is no link between entering personal information banks for tracing purposes as opposed to entering personal financial records is questionable *

* In the United States the federal government now has agreements with leading credit bureaus in the private sector to help trace delinquents for federal debts other than tax debts.

- . It is not yet clear whether any information collected for tracing and seizure purposes will be made accessible to the individuals affected
- . A special exemption is applied in certain designated law enforcement situations, for example, to prevent tracing (or at least identifying) informers.

The attempt to go the legislative route, to restrict how the State gains access to personal information for purposes other than it was created, turns out to be another means of undermining the Privacy Act. *

Law Enforcement Agencies and Personal Information - Section 8(2)(e)

Sections 8(2)(c) to (f) primarily allow certain law enforcement agencies access to individual information. Section 8(2)(e), in particular, is drafted broadly, without sufficient reference to statutory authority, clearly designated law enforcement personnel, or informing the individual affected of such entry. There is no provision, as there is in the Canadian Security Intelligence Service Act for example, for such access to be granted in all cases only after a judicial information warrant is issued, specifying the reasons for which the information is needed. There is also no provision for notifying individuals about such entry, unlike the 1974 Protection of Privacy Act which stipulates that individuals must be notified after the fact of a wiretapping incident. **

* The Privacy Commissioner privately submitted his views on the family orders maintenance legislation to the Justice and Legal Affairs Committee of the House of Commons. The Commissioner's critical comments dated September 3, 1985 are now available from the Committee and the public interest would have been better served to have his comments available publicly before the divorce legislation was passed into law. The Privacy Commissioner, along with the Information Commissioner, had also submitted their critical views in private in late 1985 to the Government of Canada on the Conflict of Interest and Post-Employment Code for the Public Service.

** In the case of 17 investigative agencies from aviation and drug investigators to the RCMP identified under Section 8(2)(e), notation of entry on individual files was permitted under Section 9 of the Act. However, the Canadian Security Intelligence Service Act extinguished that right in 1984 because the 18th agency, CSIS, wanted no part of such an individual flagging system, nor did some of the other 17 investigative agencies including the RCMP

Further, access is not provided to any of the reasons why third party access was sought and approved. *

Departmental annual reports are required to report the uses made of Section 8(2)(e), yet they are not very helpful. The Privacy Commissioner is currently requesting departments to provide the details of some of these Section 8(2)(e) uses as part of an audit he is undertaking. It is hoped that he will issue a Special Report with recommendations about this section of the Privacy Act. Departments are not supposed to allow the 18 investigative agencies automatic access to their personal information holdings.

While use of Section 8(2)(e) by designated investigative agencies may not be that widespread, any use of this provision needs to be closely monitored, as does law enforcement agencies' wider use of Sections 8(2)(a) and (b) as means to gain entry to personal information. There is no requirement, as in Section 8(4) of the Act, that records be kept of investigative agencies' uses of Sections 8(2)(a) and (b) even for the review of the Privacy Commissioner. In the absence of judicial supervision, it is simply too easy for law enforcement agencies to conceal their entry and monitoring activities from individuals under the Privacy Act.

Data-Sharing Agreements Between the Federal Government and Other Organizations Under Section 8(2)(f)

Section 8(2)(f) of the Privacy Act, as it has been put into practice, provides yet another illustration of the problems of allowing law enforcement and other agencies broad and vague third party access to personal data.

* In a 1985 District Ontario Court ruling, presently being appealed by the federal government, an accused person was granted permission to access a sealed packet containing the reasons police gave a judge when they sought to tap his telephone under the protection of the Privacy Act.

Federal-Provincial "Catch-All" Agreements - Section 8(2)(f)

One major initiative undertaken at the time the Privacy Act was proclaimed in 1983, was the signing of personal data-sharing agreements by the federal Justice Minister with ten provincial Attorney Generals and with the Yukon (the Northwest Territories never signed an agreement). These agreements are essentially all the same although Quebec wanted and is renegotiating more detailed department by department agreements.

After some difficulty, this researcher obtained these unpublished agreements using the Access Act in late 1983. * A close inspection revealed that the agreements were designed primarily to allow fairly broad sharing of law enforcement and security information, although they were held up to be blanket "catch-all" controls for any kind of inter-agency personal data sharing. Documentation viewed under the Access Act leading up to the signing of the 1983 agreements indicated that Justice officials had serious doubts about the effectiveness of the agreements. Justice officials also conveyed to other federal agencies that these 1983 agreements, once they were signed, were to be viewed as minimal tools of privacy protection. **

The agreements contain vague clauses that bring into question the security of the transmitted personal information. They are quite loosely worded when it comes to describing how the collected and shared personal information will be used or re-used. No retention or disposal schedules are attached. *** The agreements do not establish any real mechanisms to police their terms or to penalize

* See Prying Eyes (1985), page 15.

** See Testing the Spirit of Canada's Access to Information Act (1984), pages 18 to 25.

*** The Privacy Commissioner, in a letter dated August 10, 1984, drew this researcher's attention to some of the concerns with these catch-all agreements he had voiced earlier in his Annual Report. He hoped that a "change of attitude" would eventually take place but stated that it was beyond his jurisdiction to review as "to whether or not there is adequate inspection and enforcement safeguards for privacy protection in these agreements".

offenders. * Further, provision was made in 1983 so that the agreements could be amended in private after 6 months without any periodic public review.

The idea of written agreements or arrangements for sharing personal information with provincial, municipal and international bodies, at least for law enforcement purposes, has the potential to be an excellent use and disclosure mechanism. The Canadian government, in not even bothering to publicize and automatically release the agreements made under Section 8(2)(f), has clearly indicated that it does not treat these agreements very seriously.

Personal Information Data-Sharing Agreements and Arrangements in General

As part of this researcher's review of Section 8(2)(f), ten departments were asked under the Access Act to disclose their own agreements under Section 8(2)(f) beyond the "catch-all" ones discussed above. Some departments responded promptly, and even provided information related to arrangements for data-sharing that in effect could be considered to fall under the broader terms of Sections 8(2)(a) or (b) of the Privacy Act. Departments like Health and Welfare initially had difficulty with the request and only after my complaint to the Information Commissioner began to respond. Some departments like Indian and Northern Affairs and the RCMP insisted that the only personal data-sharing agreements they followed were the ones Justice Canada signed in 1983.

This researcher viewed over a hundred departmental agreements or arrangements from several of the ten federal agencies. ** These data-sharing agreement contracts and letters of arrangement between the federal government and provincial or foreign governments vary

* Treasury Board guidelines of June 22, 1983 related to the establishment of further "model" agreements under Section 8(2)(f) are similarly vague and without tough enforcement safeguards.

** See Testing the Spirit of Canada's Access to Information Act (1984), pages 23 to 25.

greatly in terms of their quality and binding nature. * Most of them are quite vague and without stringent protection or restrictions on sharing personal data.

The Privacy Commissioner explained in a letter of July 9, 1984 that he saw no legal requirement to periodically publicize such agreements or arrangements even though he noted that such a list might be useful. It is the Privacy Commissioner, however, who should be notified, first, of these arrangements and other disclosure scenarios. ** There is little to prevent the Commissioner from investigating these matters or auditing third party disclosure practices.

Most annual privacy reports from federal departments are vague on third party use and do not list existing or new personal information data-sharing arrangements, or the legal authority for such arrangements.

Not all persons or groups outside the federal government (and not all officials inside the federal government) who obtain and exchange personal information are required to have agreements or public agreements. Some departments, for instance, store their personal information holdings with outside firms and check with outside groups, such as employers, for information on their employees. Some large departments, like Health and Welfare, regularly share personal information among their many social welfare and health branches and have as yet to reach arrangements, for instance, on how to share personal data with Indian and Northern Affairs on native health problems.

Section 8(2)(f), a potential tool for tightening third party disclosure, turns out in practice to be, more of a tool to facilitate greater and more continual sharing of personal data in private,

* These agreements or arrangements are not generally publicly known or listed in the Personal Information Index or on file with Justice Canada or Treasury Board.

** Under the Privacy Act, the Commissioner is notified of Section 8(2)(e) use, in cases of "public interest" (Section 8(2)(m)) and in cases of "new" consistent uses before Section 8(2)(a) applies.

without public knowledge. A special inquiry ought to be conducted to create a tighter and more precise model of what constitutes a personal information sharing agreement - a model that can apply to law enforcement personal data exchanges, as well as to other personal information transmissions authorized by statute.

Third Parties Under Section 8(2)(g),(h),(l) - Members of Parliament, Auditors and Debt Collectors

It is questionable whether some of the third parties listed in Section 8(2)(g),(h),(l) should be included under the Act and given such easy access to personal information.

It is difficult to see the validity of giving Members of Parliament special third party access rights to perform their duties, as occurs under Section 8(2)(g).

Auditors may need access to personal information in order to do their specific statutory jobs but provision for this in Section 8(2)(h) does not specify exactly who the individual auditors are and what use they can make of personal information in specific cases.

Section 8(2)(l) is broad, without any specified due process features, and simply enables federal authorities to open the door widely to debt collectors. In the United States it appears that such powers are confined to specific legislative enactments, such as the 1982 Debt Collection Act. This seems to be the approach Canada is taking, judging at least from the 1986 Family Orders Enforcement Assistance Act and the 1983 amendment to the Financial Administration Act. * It seems, therefore, that Section 8(2)(l)

* Under the 1983 amendment (Section 5(7)), the federal government is authorized to trace the whereabouts of federal employees. This amendment changed the disclosure of this personal information on federal employees from a discretionary 8(2)(l) (debt collection) situation to a mandatory 8(2)(b) (legislative enactment) situation. A separate 1983 Act, the Garnishment, Attachment and Pension Diversion Act provides the legal authority to garnish a portion of federal employees' wages, tax refunds, pensions and other monies received from the federal government for matters such as loan repayments and family support, provided court orders are secured, first.

should be deleted and only re-adopted, in specific statutory enactments, after parliamentary review if absolutely necessary.

Researchers As Third Parties Under Section 8(2)(j)

Sections 8(2)(i) to (k) allow for access to personal information for the purposes of doing archival research, statistical and general research, and native land claims research. As with the other sections of the Act related to third party access, only a few conditions have to be met in order for a researcher to gain access to information.

In the case of Section 8(2)(j), there is an explicit recognition that access to information requires a written undertaking. The written research undertaking forms I have viewed have all been rather vague. * While the penalty of not being welcome back to do further research is a type of deterrent, it is not the only means or certainly the fairest means of penalizing abuses by researchers. The deterrent is particularly unfair when such a penalty is rendered in private without due process rights and without specified access restrictions (eg. a five year cut-off period from access to "X" branch's personal information files of that department).

Research undertakings should not include prior government viewing of researchers' manuscripts and it should not be so rigid that researchers cannot examine valuable data, particularly where the individuals' consent can be or has been obtained. Researchers should not be granted special privileges, however, and should not carry on with the expectation that all they have to do is sign honour pledges in order to obtain access to personal information.

A researcher is defined in Section 8(2)(j) as "any person or body for research or statistical purposes..." and can include, therefore, many different kinds of investigators. It would be hard

* I rewrote the research pledge I signed with CMHC for two reasons: first, to protect my right to report the data I examined without prior agency approval; and secondly, to indicate clearly that I agreed not to use any of the identifiable personal information I viewed.

for instance, to exclude non-professional researchers. The possibilities for abuse are there with a wide open definition of researchers. The best protection against abuse is a set of deterrents, starting with the requirement that researchers write and sign a statement describing how they will use the requested personal data. Preferably, research will only take place after the affected individuals have been notified and have given their consent for the research.

Under a revised Section 8(2) researchers should be subject to tougher fines as well as future specific restrictions on access, with due process procedures applied, should they misuse the personal data to which they gained access.

Section 8(2)(m) - The Public Interest

The ultimate means of disclosure for third party access to personal information is created in Section 8(2)(m)(i) of the Privacy Act. In this section, "the public interest" outweighs personal privacy, subject only to the private notification of the Privacy Commissioner who may then notify the affected individuals before access to their personal information is granted.

What this establishes in effect, is a public interest override to the mandatory personal information protection clause in Section 19 of the Access Act. The problem with this "balancing test" is that it is done primarily without the affected individual's knowledge or consent. Treasury Board has proposed some guidelines on how to apply the override, but these criteria are not found in the Privacy or Access Acts. Several cabinet discussion papers from the period 1978 to 1980, which were prepared to develop improved privacy legislation, expressed the concern that if a formal balancing test between individual privacy and public access was adopted, the government and individuals could then be put on the defensive to prove their case in court that release is an "unwarranted invasion of privacy". *

* The author obtained several of these discussion papers by applying under the Access Act.

The problem with Section 8(2)(m)(i) would be partly rectified if there was a clear directive requiring that affected individuals have knowledge of or be asked for their consent whenever the balancing test of Section 8(2)(m) is applied. A clearer definition of what actually constitutes situations when the public interest override could legitimately take place would also help to protect personal privacy. * The public must be informed of all instances when the public interest override provisions can apply. Section 3 of the Act should also be re-examined so that the definition of personal information can become more reflective of the balance between openness and privacy.

Parallel changes will be needed in the Access Act, in part to amend the mandatory nature of Section 19 (personal information) of the Access Act and in part to define what constitutes a residual public interest balancing test, with similar wording hopefully adopted for both Acts. **

The balancing between privacy and openness is difficult to accomplish on a legislative basis. The protection of individual privacy should still be cardinal, but it is not helpful to have Section 8(2)(m) remain a hidden reverse privacy protection clause. *** It is much less awkward and paternalistic to have a publicly defined residual balancing test, and a means whereby affected individuals can be consulted so as to determine whether their information is or is not able to be shared with others.

* The proposed Ontario FOI Privacy Bill (Bill 34) tries to define the residual public interest balance needed.

** Refer to my report Suggested Changes to Canada's 1982 Access to Information Act (1986) for the access perspective.

*** This researcher unsuccessfully sought to examine the Section 8(2)(m) cases not mentioned in the Privacy Commissioner's annual reports. Some agencies apparently have wanted to use (dare I say abuse) the public interest override clause by declaring that whole classes of personal information not specified in the Privacy Act can be made accessible (though not necessarily accessible to all members of the public). One attempt, apparently rejected by the Privacy Commissioner, was Immigration's request in the public interest to have access to files kept by Indian and Northern Affairs on Canadian native people.

Unauthorized Third Party Access

The Privacy Act steps lightly when it comes to unauthorized third party access. The basic corrective mechanisms appear to state that once one notifies the Privacy Commissioner of inconsistent use and lists the new use in the next Personal Information Index, then the third party entry will be legal. There is no real system for judicial warrants or gaining approval for emergency, unauthorized third party access. Nor is there any mechanism in the Privacy Act to hold public hearings or inquiries about such practices. *

While penalties exist in other statutes for some types of illegal third party access to personal information banks, it is unfortunate that fines and even jail sentences, are not currently part of the enforcement means to handle unauthorized third party access.

Without tightening up the language of the Act in regard to what constitutes unauthorized third party access, penalties would be fairly useless, because legal third party entry is so prevalent under the existing Privacy Act.

Accuracy of Third Party Information

The Privacy Act does acknowledge that personal information held and used by the government should be "as accurate, up-to-date and complete as possible" (Section 6(2)) and that "reasonable steps" should be taken to ensure this; particularly since administrative decisions can be made on the basis of personal information. However, this is not the equivalent of guaranteeing the accuracy of information on file.

* The will has to be there to prevent unauthorized third party entry. For instance, the 1980 Report of the Ontario Commission of Inquiry into Confidentiality of Health Information uncovered various questionable third party abuses, including the wide use of pretext calls by certain insurance companies and lawyers to obtain medical information about accident victims. No penalties have ever been levied and no legislation has ever been introduced that effectively restricts such practices.

The problem appears to lie less with individuals not supplying accurate information about themselves, and more with third parties who provide potentially inaccurate information, or at least, hearsay that is not identified as such. The possibility that inaccurate information may be collected is only indirectly recognized in Section 5(3). The only remedy that is provided in the Privacy Act in Section 12(2) is for individuals to try to correct the information if they can gain access to court files already there. No provisions are made in the Privacy Act for an individual to sue a department that keeps inaccurate information, and no penalties are applied against departments for holding inaccurate information. *

Measuring Third Party Access

Legalized snooping is a serious problem. Its true dimension has yet to be measured. No Treasury Board figures are kept at all on Section 8(2) requests by third parties to access specific personal information banks.

Ironically, figures are reputedly kept on the requests made by outsiders for the personal information of others (but not by specific personal information bank). Treasury Board statistics indicate that departments apply Section 26, that is, they reject requests for personal information about other persons, in 45% of the cases of Privacy Act applications that were subject to exemptions.

But this is somewhat misleading because a large percentage of such citations are likely the result of departmental misuse of this exemption. ** When a record contains a great deal of personal information beyond that to which the affected individual is entitled,

* Some acts, like the Unemployment Insurance Act, do contain penalties for individuals not supplying accurate personal information.

** There are of course instances when family members, employees, marketers, neighbours and others do request personal information about someone other than themselves, and undoubtedly some requests are deliberate attempts to invade others' privacy.

many departments appear to be wrongfully citing Section 26 as if the individual was also applying for information on others. This is one reason why the severability principle should be built into the Privacy Act as well as the Access Act.

Third Party Restrictions

Third parties have too many rights:

- . They can access personal data without any penalties for misusing data
- . They can contribute to personal data files without the affected individual's knowledge (the use of informers is growing, not declining)
- . They can contribute hearsay to personal files without any penalties for blatantly providing inaccurate information .

Privacy Act users can have difficulty dealing with situations when third parties access their files:

- . They are not asked for their consent in many cases of third party access
- . They are not generally notified when third party access takes place
- . They are not always likely to find out if unauthorized third party access is approved by the Privacy Commission
- . They are not given any rights under the Privacy Act to sue for damages for inaccurate third party information or for the misuse of personal information by third parties.

In summary, tightening third party access will require the following eight measures:

- . All third party disclosures must have legislative authority conforming to a strict disclosure code
- . All third parties shall be precisely identified

- . All agreements and their amendments for personal information sharing should be made public, and should be made available for Privacy Commission hearings and Parliamentary approval
- . Third party access to law enforcement agencies should only be granted after a judicial information warrant is issued, specifying the reasons for which the information is needed
- . Third party access ought to be noted on individual files except in security intelligence cases when a court orders otherwise
- . The Privacy Act should be amended to ensure that personal data is sufficiently protected from illegal third party access *
- . Penalties for unauthorized third party access should include minimum fines of \$5,000 and jail sentences of up to five years
- . Information on personal files provided by third parties should be clearly identified as having such an origin. Individuals should be guaranteed information on them is accurate.

The limited amount of privacy protection that is afforded by the use and disclosure clauses of the Privacy Act raises significant concerns, particularly about individual control of one's own data and about third party access and procedures.

The following section of the report deals with another matter that heightens further these concerns about control over data and third party access; computer technology is being used more and more to link, match and profile, in a way that violates the limited use and disclosure provisions of the Privacy Act.

* The Privacy Act creates the illusion of secure personal information holdings without sufficient provisions for preventive safeguards or penalties to protect those holdings.

C. COMPUTER LINKING, MATCHING AND PROFILING

The designers of the Privacy Act missed an opportunity to deal with advances in computer technology which now make it possible to manipulate personal data and achieve third party access between computers.

The Privacy Act's promise was that computer as well as manual personal data-matching and linking could be controlled. The control was to come in the form of authorization and by fully describing such practices and making them public, for example, by registering these activities in existing newly created personal information banks.

At issue is whether the existing requirements of the Act can, in practice, result in the full public identification of such matching and linking; whether all existing linkages are authorized or should be; and whether unauthorized record linkages can be prevented given the emerging technology of distributed data bases, personal computers and linked microcomputers. *

Before the passage of the Privacy Act a widely debated issue was whether a person's Social Insurance Number (SIN) could become a computerized national identification number. SIN was originally used as a registration linkage number for specific social security and taxation programs, but it eventually gained widespread use as an identification number in many sectors. **

After the passage of the Privacy Act the focus was placed on computer-matching. Although this issue has not generated very much intense public discussion, some people are concerned that vast and disparate sets of personal information can be instantly searched for their similarities and differences. The result of this, in some cases, is that new personal information can be created through technological linking.

* The Privacy Act does not deal sufficiently with the matter of securing computer data so that EDP files containing personal information can be kept more efficiently.

** There are eleven federal laws or their regulations that allow agencies to request a person's social insurance number. They are the Canada Election Act, Canada Pension Plan Act, Canada Student Loans Act, Canadian Wheat Board Act, Excise Tax Act, Family Allowance Act, Immigration Act, Income Tax Act, Race Track Supervision Regulations of the Criminal Code, Old Age Security Act, and the Unemployment Insurance Act.

The Social Insurance Number Debate

Two legislative approaches were suggested in the period 1978 to 1982 to tackle the problem of an increasingly widespread use of SIN. To begin with, the Conservative government advocated restrictions on SIN usage in the seventies and, while briefly in power between 1979 to 1980, did away with its use to cash Canada Savings Bond interest coupons. The Conservatives proposed a privacy bill which was never introduced in Parliament, but which made provision to abolish the use of SIN as a registration number for the Canada Students Loan Program. The privacy bill also included the promise that the federal government would refrain from using SIN informally and would protect Canadians from losing benefits in situations where providing a social insurance number was not a requirement by law. The bill also empowered the Privacy Commissioner to hear complaints on SIN abuse.

Secondly, the Liberal government advocated the approach that legislation restricting SIN usage should not be enacted. Accordingly, the Liberal's Privacy Act did not contain any cutbacks or specific restrictions on SIN usage. Instead, the Act endorsed authorized record linkages using SIN, and it authorized certain third party access to records using SIN. While this point was not explicitly stressed in the Privacy Act of 1982, SIN usage was supposed to be registered and identified in the Personal Information Index to show that SIN was used in an authorized, statutory fashion or as part of administrative requirements. There is, however, no specific clause in the Act, for example, that requires officials to keep track of SIN usage or to document the reasons for using SIN in each case.

The Liberal government approach may have been influenced in part by the Privacy Commissioner's Inquiry Report of 1981 which warned against specifically restricting SIN usage as one form of record linkage and identifier. However, neither the Liberal government, nor the Conservative government more recently, have ever really acted on the Privacy Commissioner's solution, which was to enact Criminal Code provisions for wrongfully creating and using SIN or other record linkages.

The current Privacy Commissioner, Mr. Grace, agreed with his predecessor, Ms. Inger Hansen, that identifiers, like SIN, are here to stay as part of the computer technology landscape and that restricting SIN usage would be a band-aid solution. Although he questions the broadening use of national identifiers without public debate and sees the value in greater protection against wrongful SIN usage, Mr. Grace has taken the view that the Privacy Act does not provide him with any special guidance on the issue of SIN usage. The Act does give him considerable power, however, to influence public awareness of the issues surrounding SIN usage.

In his 1985 audit report of Fisheries and Oceans, the Commissioner failed to take a firm stand against SIN abuse. This was the case even though his report included the finding that SIN was used as an identifier for a particular personal information bank in some regions but not in other regions. Instead of offering sharp criticism, the Commissioner made the rather mild suggestions that the department consider "adopting a standard national procedure for using SIN as identification". He did add that, "If SIN is not needed, it should not be requested on application forms (i.e. applications for commercial fishermen's licencing and vessel registration)".

The extent to which SIN or other unique identifiers have been used in the public and private sectors to link pieces of personal information has not been comprehensively examined, at least publicly, since the 1981 Privacy Commissioner Report to Parliament and the passage of the Privacy Act. *

* This researcher was surprised, for example, that there was little public reaction or Parliamentary debate when machine-readable passports were introduced in the mid-eighties. The automated passports were designed to be read by computerized scanning systems at border crossings and they met the International Civil Aviation Organization's (ICA) standards. This type of identifier card is likely to give immigration, customs, and police agencies all around the world instant access to information. If many countries adopt the ICA stand and possess the needed technology, one large travel-immigration data base could be created.

In typical Canadian fashion, whenever there is a legitimate concern about privacy matters such as record linkages and the use of SIN, the issue tends to be diffused and only vague policy stands are put forward.

Technological advances may have overtaken the SIN debate to some extent in North America. In other countries like Australia and West Germany, however, the idea of having one national identifier card continues to be an extremely controversial issue.

Future SIN usage should be the subject of Parliamentary debate. Legislation ought to be enacted to restrict the use of SIN and to ensure that any approved uses are clearly authorized and identified.

Computer-Matching

The former Privacy Commissioner, made it known in her 1981 Report that she believed the record linkage debate should move beyond a concern for the impact of centrally linked computer systems storing a great deal of our personal information. Her focus of concern was the various abilities of increasingly proliferate technology to link and abuse our personal information. The current Privacy Commissioner has reinforced this concern. Mr. Grace has taken aim at the problem of knowing how much federal information is or will be accounted for and sufficiently protected, with the advent of the mini computer and other modern technology.

He has also done much to direct public attention at the problems associated with using computer technology as an investigative tool, to link or match personal information in the hope of improving the effective administration of government benefits to certain recipients. Mr. Grace has expressed concern that computer-matching may not be subject to enough safeguards and may be responsible for gradually watering down the Privacy Act.

The Commissioner's statements on computer-matching may have been influenced, in part, by the actions of Perrin Beatty, the

Solicitor General. When Beatty was an opposition M.P. in 1983, he complained to the Privacy Commissioner about a request made by some officials within his department. They wanted to manually cross-match automated, financial data from the City of Kitchener with tax information on file in the department in order to try and identify potential tax cheaters.

This researcher explored the state of Canadian computer-matching in 1984 and found that the issue did indeed warrant public and Parliamentary debate. * My findings indicated that the scope of federal computer-matching is considerably greater than that envisaged in the Revenue Canada-Kitchener situation. The federal government has used computer-matching in at least the following three ways:

1. To Catch Individuals Who Cheat the Social Welfare, Tax and Family Maintenance Systems
 - . Canada Employment and Immigration has made use of several cross-matching programs designed to catch UIC cheaters. These include running federal unemployment insurance claimant computer records with provincial welfare records and matching UIC claimant records with employment separation and report on hiring records. The proper implementation of many of these programs depends on the cooperation of private sector employers.
 - . Revenue Canada has run computerized hotel tapes through Ottawa's tax computer systems to see whether the figures tallied with income reported by waiters and waitresses.
 - . Parliament introduced a federal matching program proposal to help trace family maintenance defaulters and people who wrongfully abducted their children.

* See "No More Cheating - 1984 Style" in Essays on Privacy Invasion (1985).

2. To Trace Legally Recognized Debtors

- . In 1983, Parliament amended the Financial Administration Act to allow the release of addresses of federal public employees and to allow the seizure of federal monies received by these employees in cases of court ordered garnishment.

3. To Profile, Locate and Monitor Security Risks

- . The 1974 Canadian Security Intelligence Service Act allowed security agents to engage in secret computer runs once judicial warrants were issued.

Computer-matching activities are also quite prevalent in the private sector for such purposes as credit granting and market profiling, even though the general public is not always aware of or knowledgeable about these practices.

It is difficult for someone who is not employed by the government to discover the extent to which computer-matching is done. It was not until 1985 that Treasury Board conducted an unpublicized survey of the manual and computer-matching and linking practices of 12 government institutions that controlled large holdings of personal information. Treasury Board's Report of March 1986 to the Justice and Legal Affairs Committee indicated that the agencies in the survey carried on "a considerable amount of data-matching" (page 25).

This researcher informally obtained a summary of the survey replies from Treasury Board. Eleven of the twelve agencies reported 85 existing and 4 planned linkage practices. * The twelfth agency, the RCMP, did not provide specifics. Social insurance numbers were used to link data in 72 of the 89 existing and planned linkages. Computers were used to do the linking completely in 53 cases and partially in 7 cases; the rest of the linkages were done manually.

* Canada Mortgage and Housing Corporation (3, one planned), Employment and Immigration (13, one planned), External Affairs (1), Health and Welfare (41), Labour (nil), Public Service Commission (2), Revenue-Customs (2), Secretary of State (1), Statistics Canada (2), Supply and Services (20), and Veteran Affairs (2 planned).

Over one-half of the linkages resulted in the creating of new personal information. Only a third of the agencies bothered to file a report on these linkages in the Personal Information Index. Agencies claimed data-matching was done as a "consistent use" or under the authority of Section 8(2) of the Privacy Act.

Some of the linkage practices that were reported in the Treasury Board survey summary included immigration control, UIC and disability pension matching, tracing old age security recipients for over payments, air pollutant comparisons using school children, and matching Customs and RCMP files to build intelligence information on potential customs offences.

It is likely that not all of the linkage practices were reported in the survey and, certainly, not all the federal agencies with large personal information holdings were actually surveyed. Indeed, Treasury Board acknowledged that the institutions it had surveyed had largely "failed to account for matching activities properly, as required by the legislation".

Treasury Board recommended that agencies should be held to the following three requirements:

- "a) to describe all matching activities and the type of information resulting from the match;
- b) to register any new bank resulting from data-matching and
- c) to report in sufficient detail to clearly identify the authority under the Privacy Act permitting the match."

These recommendations are inadequate because they do not include ways to restrict computer-matching and they imply that agencies' data-matching activities are adequately covered under the existing use and disclosure policies of the Act. Whereas Treasury Board focussed on the failure of agencies to examine or report their matching against policies in the Act, this author

believes that the problems lie more with the Act itself rather than with the reporting practices of the agencies.

The Privacy Commissioner, in a letter of findings to Perrin Beatty, for example, on the Revenue Canada-Kitchener complaint case, suggested that there was a crucial need for specific use and disclosure guidelines for computer-matching. * The Commissioner made the following recommendations:

- . Computer-matching should not be used to extract personal information that does not have anything to do with the purpose of the match
- . Any personal information collected as a result of a computer-match should be retrievable and, as a general rule, accessible to the public
- . Computer-matching should be covered by agreements that set forth the use for which the information is collected
- . Where feasible, the fact that computer-matching may take place should be made known to persons surrendering their personal information in the first place
- . Some independent authority should be notified of proposed matches and made aware of the methodology under which computer-matching is conducted.

The Commissioner's guidelines on computer-matching are a starting point but they do not sufficiently address five important issues: **

- . Is computer-matching a violation of the Privacy Act?

* The letter was dated May 1984 and was released by Mr. Beatty. It is worth noting that the Quebec Commission d'accès à l'information has also been developing computer-matching guidelines.

** Some of these issues were raised by participants at an October 1984 Science Council of Canada Privacy Workshop and by witnesses at the 1982 American Congressional hearings on computer-matching.

At issue is whether the computer-matching done on a case-by-case basis is a form of indirect collection of personal information authorized under Sections 5(3) or 8(2) of the Privacy Act. Treasury Board itself recognizes that some of the current matching may not have met the Act's collection, use and disclosure policies.

- . Is computer-matching adequately covered under the Privacy Act?

Computer-matching practices were not envisaged when the collection, use and disclosure policies of the Act were drawn up. This was the case despite the fact that the authorities were aware at the time that the issue was a controversial one in the United States, as Congressional hearings of 1982 had stirred up interest in the growing federal and state use of computer-matching. It is very legitimate to question, therefore, whether Sections 5(3) or 8(2) of the Privacy Act, or other sections of the Act, can cope with computer-matching practices.

- . Is computer-matching an effective and necessary investigative tool?

Computer-matching may well allow for a fast comparison of personal information but it may not always prove to be the best investigative tool for every situation. Some think it may be better to collect information directly from individuals or to rely on less expensive means of collecting information; computer-matching, in other words, does not always produce accurate findings and it is not always cost effective.

For instance, the electronic tracing by the government of family maintenance defaulters and child custody abductors is unlikely to be the main method of tracing such people and some would suggest its effective use is only as a last re-

sort tracing method. Others, like the Canadian Council for Co-Parenting challenge the need for widespread electronic tracing because they see the answer lies in the State encouraging solutions such as co-parenting custody to prevent financial problems caused by family separation.

- . Is computer-matching a new search and seizure tool that is used without consideration to due process, without public knowledge, and without the application of constitutional safeguards?

Computer-matching can permit government to engage in widespread "fishing expeditions". A 1985 study, Search and Seizure Under the Income Tax Act, by Neil Brooks and Judy Fudge of the Law Reform Commission, described the broad search and seizure powers of the Income Tax Act. The authors expressed the hope that a proper balance could be achieved between the two concerns of providing for "greater protection to the privacy interests of taxpayers" and providing for "effective monitoring and enforcement of revenue-raising legislation".

This researcher has discovered that computer-matching can involve the practice of linking the records of thousands of innocent people who are unaware of the fact that their personal employment data is being used. This is the case, for example, at Canada Employment and Immigration where records of unemployment insurance recipients are matched with the hiring reports of private employers in order to try and catch people who are cheating the unemployment insurance system.

Concern has also been raised by David Flaherty, a University of Western Ontario professor specializing in privacy issues, about the computer surveillance via the Canadian Police Information Data Bank (CPIC) of individuals suspected of criminal activity who have committed no specific offence

and for which there are no outstanding warrants. * The CPIC bank can contain information on these individuals' known associates, aliases and personal identifiers including automobile licence plate number. The Globe and Mail (April 11, 1986) estimated that there are some 1600 individuals under observation whose movements can be monitored via the CPIC computer system to which various police forces have access. **

The RCMP, that coordinates CPIC, refuses to guarantee the accuracy of this observation data as well as large numbers of criminal records CPIC holds. *** The RCMP has to date not publicly admitted CPIC is used as more than a record cross-checking system and not openly discussed the technical and constitutional problems that CPIC or its other automated criminal intelligence systems have. CPIC cannot simply remain a self-regulated data bank without outside public scrutiny.

- . Is computer-matching an administrative or a political tool?

Computer-matching can be used as a tool to help prevent fraud, waste and abuse; alternatively, it can be used for manipulative reasons such as public relations, control of dissidents, and revenue recapture. And even in relation to preventing fraud, computer-matching can be used more to prevent low-income fraud rather than upper-income or corporate fraud.

-
- * CPIC contains mainly various criminal record or stolen property information which can be used by approximately 2500 police forces. There are some 1.3 million personal individual entries in the CPIC data bank. CPIC has a 26 member advisory policy committee consisting of representatives of federal, provincial, and local police forces.
 - ** The CPIC system, however, is not technically set up to trace individual authorized investigators who use CPIC should abuses in use of the information in the system occur.
 - *** The American Civil Liberties Union has publicly presented cases where criminal information contained in the automated National Crime Information Centre data bank has led to several wrongful arrests and detentions in the United States.

Computer-matching then, is not a "neutral" tool. Its social use ought to be assessed. To take a concrete example, in the case of catching family maintenance defaulters the State has turned itself into an electronically motivated tracing agent. One might argue that in so doing the State is reflecting public demands for fair treatment in cases of separated family units. Alternatively, the computer-matching system may have been adopted simply as a means of saving the extra costs of support and the potential loss of revenue.

Computer-matching is but one type of investigative tool adding to the information pot that can pose problems for our civil liberties. A cause for concern is the security agents' practice of computer-matching personal data after judicial warrants are granted. Another concern should be what security agents do with personal information they collect and deposit into largely exempt personal information banks, especially in cases where the information was collected before their mandate began and without judicial order.

The problems with computer-matching in comparison to other problems posed by modern electronic surveillance should not be over-blown. Nevertheless, they should be scrutinized and they should be made the subject of immediate public debate and legislative action. This researcher suggests the following four recommendations to restrict the use of computer-matching:

- . Licencing computer-matching and profiling against such criteria as cost effectiveness, necessity as an investigative tool and due process guarantees
- . Penalizing institutions that abuse publicly approved agreements to do computer-matching, and creating legal remedies for individuals who wish to claim damages for such abuse

- . Recording the use of computer-matching on individual, personal information files *
- . Clearly identifying all instances of computer-matching in the Personal Information Index. This would include listing the names of all the institutions involved in the transactions, identifying the names of all the personal information banks used; and explaining the reasons for doing the data-matching in the first place.

Computer record linking is on the increase, and more public knowledge about its use is urgently needed. Tougher regulation than is now possible under the Privacy Act is also required. The will must be there to restrict computer linkages that identify, trace, monitor, and match personal information that belongs to individual Canadian citizens.

* The technology does not leave audit trails very often and it is insufficient to simply notify the Privacy Commissioner of computer-matching usage or to record such usage on the next Personal Information Index.

PART II: BEYOND PRIVACY ACCESS AND DATA PROTECTION -
SUGGESTIONS FOR AN OMNIBUS PRIVACY PROTECTION ACT

A. BROADER PRIVACY CONCERNS

Computer technology is not a passive storage media, but an active transmission system that can be merged with other means of electronically monitoring our personal lives. For example, voice activated computers can read personal conversations; a computer work station or interactive video cable system can record personal habits; and a micro computer can call up, create, and manipulate all kinds of personal data.

Technology plays no favourites. It is not concerned with factors such as: traditional legal distinctions between oral and written communications; the distinction between a person's home, workplace and community; the way personal information is recorded; and the extent to which personal data is obtained while in transmission or from terminals. The distinction between eavesdropping and access becomes blurred. Technology is equally adept at locating debtors or creating individual marketplace profiles.

The federal government has realized the potential of the new technology to some extent in recent legislative and policy enactments. For example, the government supports the following programs or practices:

- . The electronic tracing of debtors, including public employees and family maintenance defaulters
- . Computer-matching to prevent unemployment insurance and tax fraud via computer-matching
- . The secret gaining of access to electronic mail, computer profiling and various technological surveillance means, by security intelligence agencies

- . Federally funded electronic surveillance experiments, including one National Research Council grant that deals with the use of electronic bracelets to follow the movements of senior citizens
- . Compulsory urine tests to detect illegal drug use in the Canadian Armed Forces. These tests are likely to begin in the summer of 1986, on a random spot-check basis. *

Not all such policies are new. The 1974 Protection of Privacy Act (clearly a misnamed law) legalized law enforcement electronic eavesdropping, including so-called telephone service monitoring to surveil individual worker's performance. Under this latter guise, for example, various unemployment insurance and taxation officials who deal with the public have been subjected to telephone service monitoring without necessarily having given their individual consent. **

A 1986 Law Reform Commission study on the 1974 wiretap law indicates that too many wiretaps are authorized by judges. The study is entitled Electronic Surveillance and it was prepared by

* Note that the accuracy of urine tests has been put into question in the United States, where the use of these tests has been growing. The Canadian Armed Forces has the ability to use its computer technology to store and instantly retrieve information on which personnel must submit to testing, which personnel must be disciplined, and which must be sent for treatment. A preliminary blind urine test has already been done at the Borden base where Armed Forces personnel were not required to give their names.

** Revenue Canada-Taxation in reply to an Access Act request by the author, states that after 1983 it did not engage in such telephone service monitoring (a 1% random monitoring of incoming taxpayers enquiries was done before 1983) because it received legal opinions that it was vulnerable to charges being laid against them. The documents obtained from Revenue Canada indicated that they still would like to amend Section 178.11 of the Criminal Code (that forms part of the Protection of Privacy Act) to give them a clearer right to engage in the telephone service monitoring. Other employers like Bell Canada and CP Air still use telephone service monitoring believing they have found a way around very strict individual case-by-case consent requirements as the only restrictions placed on such worker's surveillance.

Marc Rosenberg and David Watt. The authors recommend that further restrictions be placed on legal wiretapping because it is possible today to make use of the most modern technology which can record telephone conversations 24 hours a day and act like a "huge electronic vacuum cleaner, indiscriminately sucking in the relevant with the irrelevant without distinction".

The Law Reform Commission's study also indicates that the 1974 wiretap legislation has actually permitted officials to intercept private conversations of individuals who were not mentioned in judicial warrants and whose identities were previously unknown to the police. Part of the problem, according to Rosenberg and Watt, is that the public lacks information and knowledge about how this earlier electronic surveillance law works.

It can be argued that rather than being concerned about protecting Canadians from advances in electronic technology, the pendulum of government concern has swung away from privacy protection. After public controversy and a Commission of Inquiry that investigated RCMP wrong-doings, the federal government still went ahead and created a civilian security services force with immense legal powers of privacy invasion through the use of technologies such as gaining access to electronic mail and computer cross-matching. Furthermore, the legislative motion to restrict the use of federally issued social insurance numbers never came to a vote in Parliament, even though it had been preceded by considerable public and parliamentary discussion about SIN's proliferation and its growing use as an ID card and means of record linkage.

Privacy problems such as protecting personal financial information in the area of electronic funds transfer have also been the subject of years of study. But, again, no real public policies have been put in place to protect increasingly vulnerable financial data.*

* Beginning in 1987, Telecom Canada will institute a trial system to build a national electronic funds transfers (EFT) system. One of the goals of this system will be to develop new security levels to prevent electronic fraud. It is still unclear, however, whether this means that the privacy of individual electronic financial transactions will be guaranteed. An operational national EFT system is expected by the nineteen-nineties.

Whenever federal legislation is passed dealing with electronic abuse, the privacy considerations of individual Canadians is always a secondary consideration. Criminal Code amendments in 1985, for example, made illegal computer access a criminal offence. But, the intention was more one of protecting commercially sensitive information rather than ensuring high priority to securing personal information.

Canadians can hardly be forgiven for being skeptical when recent legislation actually permits the practice of mail opening, rather than clearly prohibiting such privacy invasion. *

B. A GENERIC APPROACH

Canadians have shown in recent polls that they have a growing awareness of privacy matters and an increasing impatience and cynicism with existing privacy protection policies. Canadians have not, however, united to press for better privacy protection. In fact, it is still very difficult to create a well-organized constituency around privacy issues. **

Canadians would likely prefer a broader generic approach to protect their identities and transactions. Such an approach might include the following factors:

* At least two laws, the 1984 Canadian Security Intelligence Service Act and the 1986 Customs Act, allow access to manual and electronic mail, provided certain conditions are met. Security agents performing security surveillance duties can open mail provided they obtain a judicial warrant. Custom officials can open mail provided it is suspicious international mail containing goods referred to in the Customs Tariff or any goods the importation of which is prohibited, controlled or regulated under any other Act of Parliament. Finally, mail items weighing 30 grams (the equivalent of about 11 sheets of paper) or less can be opened if the addressee or the sender consents. The provisions in the Criminal Code making mail opening and illegal computer entry a criminal offence in all other cases are not specific enough or designed sufficiently to deal with illegal entry to electronic mail.

** Most Canadians are well aware of the constitutional and charter debates of the early eighties, but they are not very familiar with David Crombie's failed attempt, in January 1981, to enshrine the right to privacy in the Canadian Charter of Rights and Freedoms.

- . It would be equipped to deal with public and private sector privacy invasion problems
- . It would take a tough regulatory approach to privacy invasion, whether the invasion was territorial or informational, written or oral in nature
- . It would place a great deal of emphasis on prevention and public education
- . It would result in greater federal-provincial, coordinated action.

Restricting the electronic monitoring of individual workers, for instance, would require a combination of voluntary and public sector strategies including:

- . Legislative prohibitions - amending labour codes, human rights codes, and the Criminal Code
- . Collective bargaining prohibitions - unionized employees negotiating the end to electronic surveillance
- . Gaining access to any employee records, including electronically created ones
- . Creating licences for electronic surveillance systems
- . Seeking cease-and-desist orders and damages through the courts
- . Joint labour-management committees on electronic surveillance
- . Union "data-stewards" to monitor the use of surveillance equipment
- . Union control of surveillance equipment used for health and safety reasons, e.g. when employees handle toxic materials.

A broader privacy protection strategy would have to include the following factors:

- . Limitation of the search and seizure powers of various federal agencies *
- . Prohibition of the close electronic monitoring of work
- . Greater restrictions on wiretapping
- . Clearer legislation that prohibits third party access to the mails
- . Prohibition of the use of lie detectors for hiring and promotions, criminal investigations and in other situations
- . Tighter prohibitions on illegally intercepting and manipulating personal information data **
- . Protection of personal information in electronic banking, credit and other financial transactions
- . Guidelines on the marketing uses of subscriber listings and profiles created from interactive video-text networks or similar systems.

The best approach would be to incorporate these measures for privacy protection into one omnibus bill.

In order to facilitate and enforce privacy protection, it would be important to have a Privacy Commission, working in tandem with the voluntary sector and provincial authorities and a vigilant Parliament.

An independent three-person Privacy Commission would need to be appointed by Parliament for five year terms (renewable once) on a staggered basis. ***

* Section 8 of the Canadian Charter of Rights and Freedoms will help reform the various administrative and statutory practices of search and seizure.

** The 1985 Criminal Law Amendment Act (Sections 46 and 58) begins to deal with the problems of unauthorized computer use and tampering with computer data.

*** One Commissioner could not adequately handle the expanded functions proposed for the Privacy Commission. Leadership can come the Commission headed by more than one individual.

The Commission's function would include:

- . Mediating complaints on privacy invasion
- . Ordering public and private sector agencies within its jurisdiction to cease and desist unwarranted invasions of privacy
- . Auditing and approving institutional privacy protection codes
- . Monitoring and reporting on the effects of information technology developments on privacy
- . Holding hearings on privacy issues
- . Reviewing proposed legislation for its privacy implications
- . Promoting privacy awareness and conducting special privacy studies
- . Providing assistance to the voluntary sector in its efforts to establish privacy protection codes.

The Privacy Commission would have to work closely with similar provincial authorities (Quebec is the only province that has the beginnings of such an authority) and groups in the voluntary sector, including industry, labour, professional, educational, media and community bodies.

The Commission ought to have a small staff and not be allowed to spawn a large bureaucracy of its own. It should focus on taking the lead in encouraging privacy protection. At the same time, however, the Commission would need to have a set of enforcement tools so that it could fully provide that leadership. It should not be a heavy-handed regulatory body, spending much of its time issuing licencing approvals of the many personal information holdings found in the public and private sectors under its jurisdiction. Rather the Commission would be most useful if it devoted much of its energy to obtaining a commitment from governmental and non-governmental groups to enact privacy protection codes. Another important task would be that of assisting individuals or groups to deal with instances of privacy abuses.

Given the nature of our parliamentary system, Parliament cannot be a passive enacter of privacy protection legislation. By creating a statutory obligation for a permanent Standing Committee on Privacy, with broad terms of reference, Parliament can itself play an active role in privacy protection.

The mandate of a Parliamentary Privacy Committee would include approving the Privacy Commission's annual budget and assessing the annual reports of the autonomous Privacy Commission. The mandate would also involve hearing from individuals and groups with privacy concerns. As well, the Committee should assess the privacy implications of legislative proposals, and conduct, at least once every five years, a statutory review of the envisaged Privacy Protection Act and its operations.

To assist the Committee in the latter role, an independent non-governmental body of inquiry should submit a report at least every five years on privacy problems and their resolution.

Such an independent body would be needed to keep track of developments in electronic technology that affect the Privacy Act and the privacy of Canadians. The inquiry body would include experts and lay people drawn from different sectors.

The assertion of privacy rights by individuals is vital to a comprehensive generic approach. Attitude and initiative are important factors that contribute to the success of providing privacy protection. The State can help through omnibus statutory legislation and the leverage and political will implied in adopting a constitutional right to privacy.

The commitment of the voluntary sector to privacy protection is a critical component of a generic approach (e.g. an individual rather than the government can sue for specific privacy invasion); but so is the commitment of government (e.g. the government can legally enable an individual to sue for privacy invasion).

Combatting privacy invasion is a means of humanizing the micro-technology revolution. The act of asserting privacy is not meant to be a rejection of the "wired-city" concept. Rather, it should be seen as an act of fighting back against electronic snooping and surveillance and trying to survive in a changing environment.

CONCLUSION

The goal of improving our Privacy Act may be difficult to achieve all at once. But much can be done right now. For example, by establishing a strong Privacy Commission, a strong Parliamentary review committee, and an independent body mandated to examine the privacy legislation every five years, we could proceed quite quickly to changing what is now a limited privacy access act into a tough privacy protection act.

Canada's 1982 Privacy Act is seriously flawed. It creates too many restrictions on obtaining access to one's files; it poorly defines personal data collection and third party use; and it does not provide a strong response to the ability of electronic technologies to manipulate personal information.

To summarize, this researcher believes that nine major changes ought to be made in Canada's Privacy Act. The Act should be amended to include each of the following provisions:

- . The registration and regulation of private sector as well as public sector personal information holdings
- . Restrictions on the amount of personal data that can be exempted
- . Tougher ground rules to ensure that only necessary personal information is collected
- . Tighter preventive safeguards restricting third-party access to personal information
- . Strict guidelines on any authorizations for computer record linkages, matching and profiling in both the public and private sectors
- . An extension of privacy protection to prevent unnecessary invasions of personal privacy in the home, in the workplace and in the community, including strict rules on electronic monitoring and surveillance of individuals

- . The Parliamentary appointment of a three-person Privacy Commission to regulate privacy protection with public input
- . The creation of a separate, permanent, Parliamentary committee on privacy to annually assess the Privacy Commissioner's budgetary needs, to examine the privacy implications of proposed federal legislation, and to hear from interested parties about various privacy problems and their resolution
- . An independent body of inquiry to conduct major reviews of federal privacy policies and practices at least once every five years.

APPENDIX ONE - The Need For a Periodic Report Card on the Administration and Operation of the Privacy Act

To date, no one has thoroughly evaluated how the Privacy Act is being administered by the institutions with responsibilities under the Act and how it is being used by the general public.

Departmental Privacy Act Administration

The only official assessment of departmental operations comes from the Privacy Commissioner's Annual Report, in which there are brief descriptions of some users' complaints against departments. The required departmental annual reports to Parliament do not shed much light on how well the departments have carried out their duties related to the Act. Most commentators believe that public employees share a growing awareness of privacy matters but also that department officials readily apply the Act's exemptions and tend to use personal information for administrative purposes in a very broad albeit authorized fashion.

Privacy Act Users

Official knowledge about Privacy Act users comes primarily from three sources: the Treasury Board statistics, the Privacy Commissioner's reports on complaints and the cases filed in Federal Court. Commentators agree that there is limited public awareness about the Privacy Act. From complaints and court cases, it has become public knowledge that only a minority of Privacy Act users have concerns about the operations and limitations of the Privacy Act, including matters such as time delays and exemptions.

Privacy Commissioner

Information on the Privacy Commission can be found in Mr. Grace's Annual Reports and speeches and, to some extent, in the

complaint case summaries he has handled which are kept internally in the Library of the Office of the Privacy Commissioner.

Outside evaluation of the Privacy Act has primarily focussed in on the Privacy Commissioner's Office. Commentators, as indicated in this report, have had mixed things to say about the Privacy Commissioner's effectiveness as an ombudsman, especially in terms of the way he has handled several cases and the way he has alerted the public to privacy concerns.

The Federal Court of Canada

Information on the Federal Court's role in the administration of the Privacy Act comes from the Court's own documentation, and from Justice Canada's Communique, a newsletter produced by the Information Law and Privacy Section.

Commentators, based on the limited Court experience to date, have tended to reflect on the Ternette case in particular. The decisions in this case have helped to force a reevaluation of the Canadian government's position on privacy matters and the Privacy Commissioner's role in handling cases of complaint.

General Comments on the Basis of Assessing the Privacy Act in 1986 and Beyond

The Parliamentary review committee does not have plans for extensive research and review of Privacy Act operations. It has retained the services of only one expert in the privacy field and it will undoubtedly have difficulty soliciting and obtaining evaluation from individual users. In addition, it will be possible for the Parliamentary committee to question departments but, as was discussed above, departments have thus far only provided superficial data on their operations.

Much of the information that the Parliamentary committee will use to assess the Privacy Act, therefore, will likely come from the Privacy Commissioner. Justice Canada officials may collect some data for the Parliamentary committee, but it probably will not be all that useful for evaluating the Privacy Act. No outside body has conducted or been asked to conduct any major research exercise or inquiry into the Privacy Act operations.

Parliamentarians responsible for changing the Privacy Act will have to rely on limited written assessments and be more dependent on the strengths of what is said by interested parties appearing before the Parliamentary committee. These interested parties in most cases have definite biases, which may make what they say of limited use. As well, Parliamentarians themselves will have their own political goals and realities which will help determine how they view changes in the Privacy Act.

Without the backup of an independent and comprehensive assessment of the Privacy Act, it may be difficult to expect that Parliament will make the necessary changes to tackle the privacy problems Canadians are experiencing.

In the United States the Congressional Office of Technology Assessment and, formerly, the Privacy Protection Study Commission, have reported on privacy problems. They have helped to provide a solid basis for a legislative privacy protection program as one realistic means of enriching future assessments of privacy legislation.

A combination of this inquiry approach with input from a concerned public and the strong political will to protect privacy are the dynamics that are needed to put the privacy protection issue well beyond the agenda of various administrators, law enforcement officials and others who want to protect the status quo.

APPENDIX TWO - PRIVACY ACT PROBLEMS FORMALLY BROUGHT TO THE
PRIVACY COMMISSIONER'S ATTENTION AND HIS RESPONSES.

January 25 , 1984

John Grace
Privacy Commissioner
Ottawa, Ontario

Dear Mr. Grace:

I found our meeting on January 12, 1984, that reviewed my study, Prying Eyes and my August 29, 1983 complaints useful.

In connection with the complaints, I would like to take the opportunity to request an investigation of them under Section 29 of the Privacy Act.

These complaints dealt with six matters:

- the lack of a complete list of federal statutes that allows third party access under Section 8(2)(b).
- the lack of a complete list of investigatory agencies that operate under Section 22(3)(a) and (b).
- the lack of an up-to-date list of all existing written agreements between the federal government and outside bodies required under Section 8(2)(f) or any procedures to periodically make such agreements publicly available.
- the questionable status of National Defence personnel information bank on Military Policy Investigation Files (ND-P-P44) as a totally exempt bank under Section 18 of the Privacy Act.
- the questionable status of Canada Post Corporation personnel information bank, for both the public and personnel - for Postal Related Crimes and Offences (CP - P20; CPC - P-P10) as a totally exempt bank under Section 18 of the Privacy Act.
- the lack of sufficient description, at least by number of files held, in the 1983 Privacy Index for 16 of the 19 exempt banks.

I would like to add, under Section 29, to the above complaints, based on research work undertaken in Prying Eyes, three further complaints:

- the lack of mention in the Privacy Index of a personal information bank, containing personal information on Canadians, for the Communications Security Establishment Agency.

.....cont'd.

- the failure to list, as specifically as possible, all federal personal information holdings of the 142 federal agencies under the Privacy Act in the Privacy Index, particularly departmental "classes of personal information".

- the inadequate inspection and enforcement safeguards for privacy protection in the model personal-information data sharing agreements (that also establish federal-provincial law enforcement and investigations agreements) initiated without publicity by the Minister of Justice under Order-in-Council 1983-1834 (June 23, 1983).

These complaints are matters that effect requesting and obtaining access to personal information. They are matters that also effect the use or disclosure of personal information. They finally are matters that effect the claims put forward for the Privacy Index under Section 11 of the Privacy Act.

I will cooperate fully in any investigations undertaken. My complaints relate to matters that should be resolved for the purpose of the Privacy Act to be carried out and not placed in jeopardy.

Sincerely,

Ken Rubin
68 Second Avenue
Ottawa K1S 2H5

(613) 234-2808



Office of the
Privacy Commissioner
of Canada

Ottawa, Canada
K1A 1H3

Bureau du Commissaire
à la protection de la vie privée
du Canada

May 9, 1984.

File: 5100-918/83

*Received
May 14/84*

Mr. Ken Rubin,
68 Second Avenue,
Ottawa, Ontario.
K1S 2H5

Dear Mr. Rubin:

In my letter of April 30, 1984, I mentioned my hope that I would soon be able to inform you about our findings in respect to the lack of a listing in the Personal Information Index covering personal information about Canadians held by the Communications Security Establishment. I am now able to do so.

As you may know, the CSE falls under the Department of National Defence. It does have, however, both unique and generic responsibilities to other government departments consistent with its mandate. The original publication of the Personal Information Index, as you correctly informed us, did not include any listing for personal information this agency collects or uses. Therefore, your complaint to us is considered justified.

You might be interested to know that DND informed us it had realized its omission and was, prior to our representation, taking the necessary steps to list a personal information bank maintained by CSE in the next publication of the Personal Information Index.

Your alertness and interest continue to be appreciated. Thank you for bringing this matter to my attention.

Yours sincerely,

John W. Grace,
Privacy Commissioner.



Office of the
Privacy Commissioner
of Canada

Ottawa, Canada
K1A 1H3

Bureau du Commissaire
à la protection de la vie privée
du Canada

July 9, 1984

Mr. Ken Rubin
68 Second Avenue
Ottawa, Ontario
K1S 2H5

*received
July 12/84*

Dear Mr. Rubin:

There appears to have been some misunderstanding in the matter of providing you with formal findings in response to the issues you raised in your letter of January 25, 1984.

I was left with the impression that you had agreed, in your discussion with members of my staff, that most of the points you had made in your letter were not of the nature to warrant a formal investigation. The exception was one complaint which was investigated and a finding made in a letter of May 9, 1984. Now you ask me to deal with your "complaints" and to make "formal findings".

My problem is that I cannot by some semantic trick turn your criticism of the Privacy Act or a representation - however specific or, even, valid it may be - into a complaint as understood in the Act.

However, and I hope this is helpful, I can respond specifically to each criticism you make of the Act or its administration. I do so, taking up your points one by one:

1. "The lack of a complete list of federal statutes that allows third party access under section 8(2)(b)".

I find no basis in law for the complaint that there is no complete list of federal statutes that deal with paragraph 2(2)(b) of the Privacy Act. While such a list may be useful for some purpose, there is no requirement in the Act that such a list be produced.

2. "The lack of a complete list of investigatory agencies that operate under section 22(3)(a) and (b)".

Paragraphs 22(3)(a) and (b) are parts of a definition section only. There is no basis in law to compel any government department to produce a complete list of the investigatory agencies to which you refer.

3. "The lack of an up-to-date list of all existing written agreements between the federal government and outside bodies required under section 8(2)(f) or any procedures to periodically make such agreements publicly available."

I find no basis in law for the complaint that there is no complete list of federal statutes dealing with paragraph 8(2)(f) of the Privacy Act. While such a list may be useful for some purpose, there is no requirement in the Act that such a list be produced.

4. "The questionable status of National Defence personnel information bank on Military Policy (sic) Investigation Files (ND-P-440) as a totally exempt bank under section 18 of the Privacy Act."

I assume that the file to which you refer is ND-P-P440, Military Police Investigation Case files, which was exempted from access by Exempt Personal Information Bank Order No. 3, SOR/83-366, dated April 22, 1983. The power to exempt banks is dealt with in subsection 18(1) which reads as follows:

"(1) The Governor in Council may by order designate as exempt banks certain personal information banks that contain files all of which consist predominantly of personal information described in section 21 or 22."

The Privacy Commissioner has no authority to receive and investigate complaints against the designation of a personal information bank as exempt.

5. "The questionable status of Canada Post Corporation personnel information bank, for both the public and personnel - for Postal Related Crimes and Offences (CP-P20; CPC-P-P10) as a totally exempt bank under section 18 of the Privacy Act."

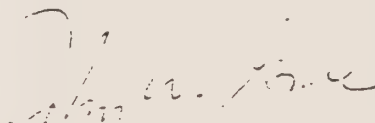
The Privacy Commissioner has no authority to receive and investigate complaints against the designation of a personnel information bank as exempt.

6. "The lack of sufficient description, at least by number of files held, in the 1983 Privacy Index for 16 of the 19 exempt banks."

There is no requirement in the Privacy Act that the number of files held in exempt banks be specified.

I hope that these responses serve your purpose.

Yours sincerely

A handwritten signature in dark ink, appearing to read "John W. Grace", written over a horizontal line.

John W. Grace
Privacy Commissioner



Office of the
Privacy Commissioner
of Canada

Ottawa, Canada
K1A 1H3

Bureau du Commissaire
à la protection de la vie privée
du Canada

August 10, 1984.

*received
Aug 14/84*

Mr. Ken Rubin,
68 Second Avenue,
Ottawa, Ontario.
K1S 2H5

Dear Mr. Rubin:

Thank you for your letter of July 20, 1984, which brought to my attention the fact that points 8 and 9 of your earlier letter were not specifically dealt with in my letter to you of July 9, 1984. I will respond to them now.

8. The failure to list, as specifically as possible, all federal personal information holdings of the 142 federal agencies under the Privacy Act in the Privacy Index, particularly departmental classes of personal information.

The Personal Information Index was published by Treasury Board. It purports to list as specifically as possible all federal personal information holdings of the agencies covered by the Act. Parliament, realizing the enormity of the task, made provision in the Act so that where discrepancies or deficiencies are discovered in the Personal Information Index, or uses for the information listed are found not to have been listed in the Index, changes can be made. I can assure you that this is being done. The Act also provides that a new Index will be issued each year. This indicates, I think, that Parliament realized that as the Privacy Act is used, changes will have to be made to the Personal Information Index. In relation to your general statement of condemnation of the Index, I am not prepared to make any finding.

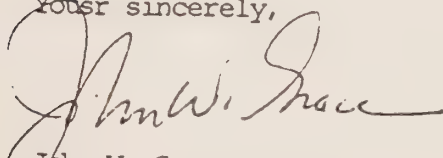
9. The inadequate inspection and enforcement safeguards for privacy protection in the model personal-information data sharing agreements (that also establish federal-provincial law enforcement and investigations agreements) initiated without publicity by the Minister of Justice under Order-in-Council 1983-1834 (June 23, 1983).

There is provision in the Act for agreements to be made between the federal and provincial governments relating to the sharing of data between these two bodies; the use of model agreements approved by Cabinet is an established custom throughout the federal government. As you will note from my annual report, I did have something to say about the type of agreements that were made with the provinces and I expect that some change of attitude will take place in the future. I cannot receive complaints as to whether or not there is adequate inspection and enforcement safeguards for privacy protection in these agreements. Though I may criticize them, as I have, the agreements themselves are beyond my jurisdiction.

You have asked if you might enter into a further dialogue in matters to which I responded in my letter of July 9. As interesting as such a discussion would undoubtedly be, I am instructed that it could be improper for me to do so.

I was pleased to hear that you enjoyed my annual report. No reader of it could have been more discerning.

Yours sincerely,

A handwritten signature in dark ink, appearing to read "John W. Grace". The signature is fluid and cursive, with the first name "John" being the most prominent part.

John W. Grace,
Privacy Commissioner.

